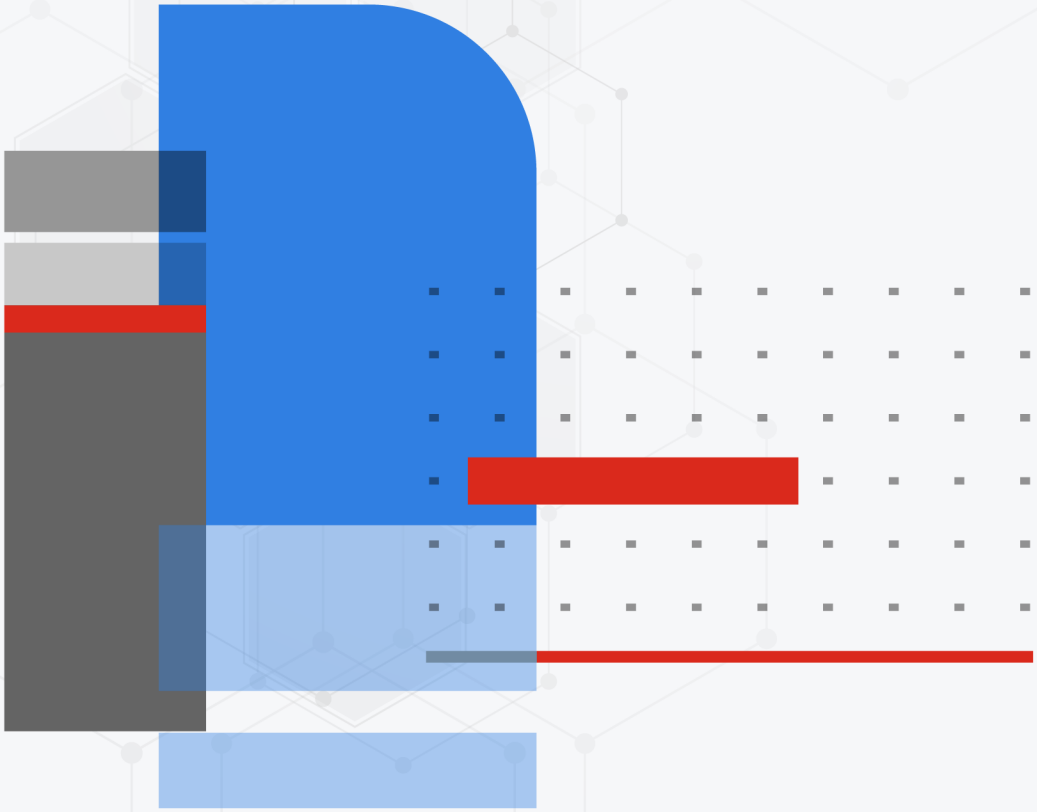
New Features Guide

FortiAnalyzer 7.4.0



FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO GUIDE
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/training-certification

FORTINET TRAINING INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://www.fortiguard.com

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

July 17, 2023
FortiAnalyzer 7.4.0 New Features Guide
05-740-898228-20230717

TABLE OF CONTENTS

Change Log **5**
Overview **6**
Fabric View **7**
Connectors 7
Webhook Connector to Support MS Teams 7
Security Operations (SOC) **9**
Asset and Identity 9
New charts in the Asset Identity Center 9
Others 10
FortiSoC GUI reorganization 11
Notifications for new Outbreak Alerts 7.4.1 14
Log and Report **16**
Logging 16
FortiAnalyzer supports FortiWeb Cloud attack logs 16
Support parsing and addition of third-party application logs to the SIEM DB 17
Per-ADOM log rate 22
Support EMS multitenancy via FortiAnalyzer ADOMs 7.4.1 24
Logging support for FortiCASB 7.4.1 26
Logging support for FortiPAM 7.4.1 28
Logging support for FortiToken Cloud 7.4.1 29
Log Forwarding 30
Fluentd support for public cloud integration 30
Reports 34
Report guidance 34
PCI Security Rating Report 36
Cyber Threats Assessment Report update 37
Threat Report update 38
FSBP Security Rating Report 40
CIS Controls Security Rating report 41
Shadow IT Report 42
FortiADC Report 7.4.1 43
Default ZTNA Report 7.4.1 45
Others 46
Time zone settings per ADOMs/Reports 46
System **50**
Others 50
FortiAnalyzer GUI enhancements 50
Fabric of FAZ topology chart 54
Fabric of FAZ: member authorization with supervisor 56
Fabric of FAZ global FortiView support 61
Fabric of FAZ: Central report support and creating Fabric groups 63
Block out contract device from upgrading to next or major or minor release 66

Cloud Services **70**
FortiAnalyzer supports FortiCare Elite Service 70
Operational Technology **74**
Operational Technology (OT) Security Service 74
OT Purdue Model in a consolidated Asset & Identity Center Dashboard 76
OT Security Risk Report 79
Index **82**
7.4.0 82
Fabric View 82
Security Operations 82
Log and Report 82
System 83
Cloud Services 83
Operational Technology 83
7.4.1 83
Security Operations 83
Log and Report 83

Change Log

Date	Change Description
2023-05-15	Initial release.
2023-05-16	Added: • Per-ADOM log rate on page 22 • Fabric of FAZ: Central report support and creating Fabric groups on page 63
2023-05-19	Added: • Webhook Connector to Support MS Teams on page 7 • Report guidance on page 34 • CIS Controls Security Rating report on page 41
2023-05-31	Added Operational Technology on page 74.
2023-06-16	Added: • FortiSoC GUI reorganization on page 11 • New charts in the Asset Identity Center on page 9 • Shadow IT Report on page 42 • Time zone settings per ADOMs/Reports on page 46
2023-06-21	Added Fluentd support for public cloud integration on page 30.
2023-06-30	Added Operational Technology (OT) Security Service on page 74.
2023-07-17	Updated Time zone settings per ADOMs/Reports on page 46.
2023-08-31	Initial release of FortiAnalyzer 7.4.1.

Overview

This guide provides details of new features introduced in FortiAnalyzer 7.4. For each feature, the guide provides detailed information on configuration, requirements, and limitations, as applicable.

The FortiAnalyzer new features are organized into the following categories:

- Fabric View on page 7
- Security Operations (SOC) on page 9
- Log and Report on page 16
- System on page 50
- Cloud Services on page 70
- Operational Technology on page 74

For a list of all features organized by the version number that they were introduced, see Index on page 82.

Fabric View

This section lists the new features added to FortiAnalyzer for Fabric View:

- Connectors on page 7

Connectors

This section lists the new features added to FortiAnalyzer for connectors:

- Webhook Connector to Support MS Teams on page 7

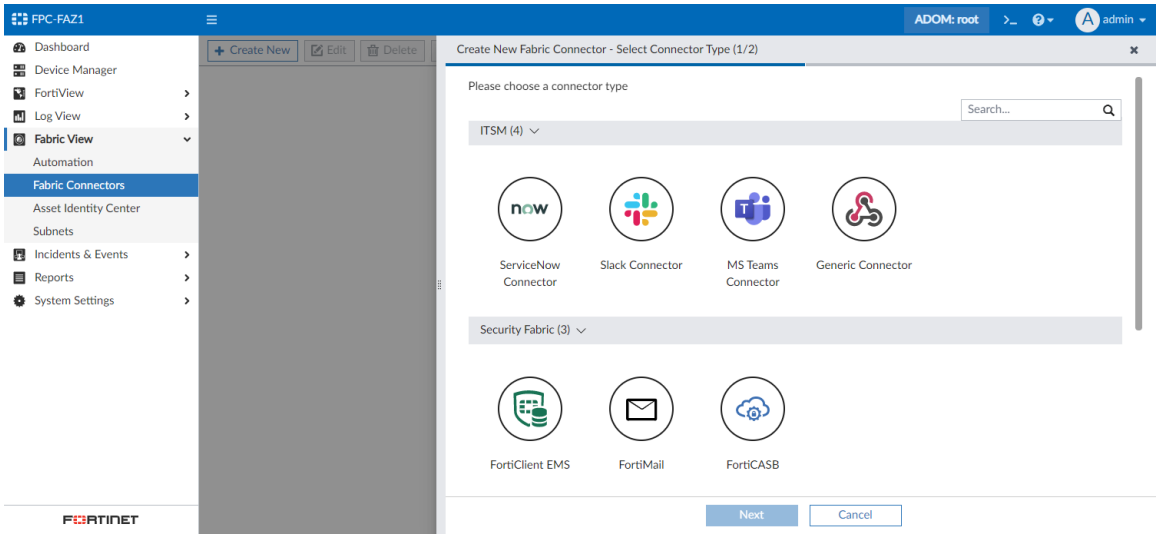
Webhook Connector to Support MS Teams

This information is also available in the FortiAnalyzer 7.4 Administration Guide:
- Creating or editing ITSM connectors

A webhook connector has been added in FortiAnalyzer to support MS Teams. This connector can be used to post a message in MS Teams.

To create a MS Teams connector:

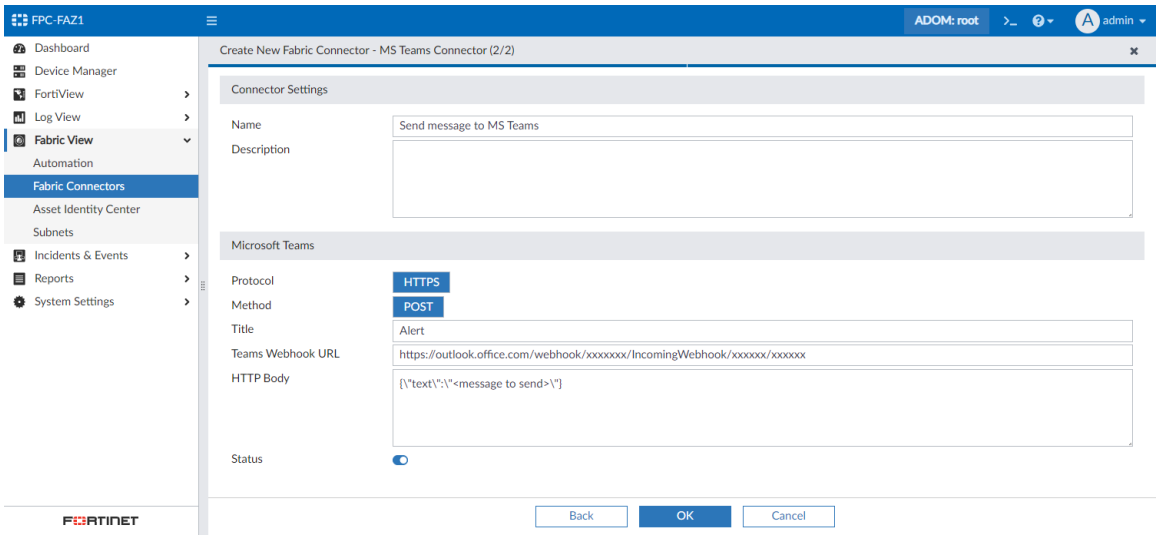
1. Go to *Fabric View* > *Fabric Connectors*.
2. Click *Create New*.
   The *Create New Fabric Connector* pane displays.



3. In the *ITSM* section, double-click *MS Teams Connector*.

4. Configure the following options:

Name	Type a name for the fabric connector.
Description	(Optional) Type a description for the fabric connector.
Protocol	Select HTTPS.
Method	Select POST.
Title	Type a title for the fabric connector.
Teams Webhook URL	Enter the incoming webhook URL created in MS Teams.
HTTP Body	Enter the HTTP body of the message that should be sent by the connector. For example, `{ \"text\": \"<message to send>\" }`.
Status	Enabled by default. The connector can be disabled, as needed.



5. Click *OK*.

Security Operations (SOC)

This section lists the new features added to FortiAnalyzer for security operations (SOC):

- Asset and Identity on page 9
- Others on page 10

Asset and Identity

This section lists the new features added to FortiAnalyzer for asset and identity:

- New charts in the Asset Identity Center on page 9

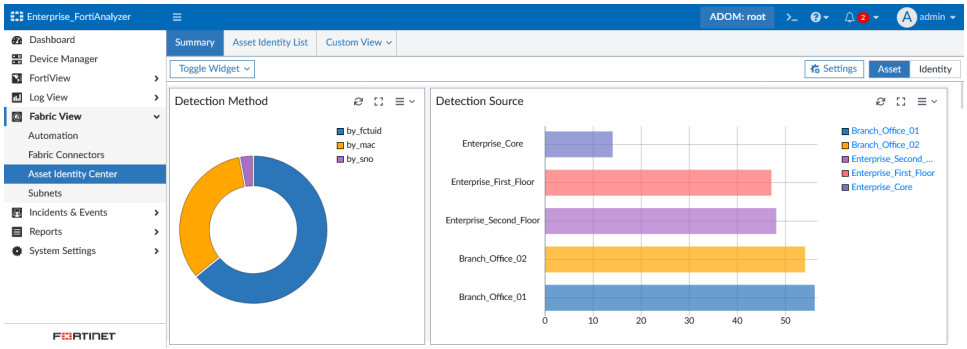
New charts in the Asset Identity Center

This information is also available in the FortiAnalyzer 7.4 Administration Guide:

- Asset Summary
- Identity Summary

The new *Asset Identity Center* pane combines the previous *Asset Center* and *Identity Center* panes. There are new and updated widgets in the *Asset Identity Center*, which can be used for analysis of endpoints and end users.

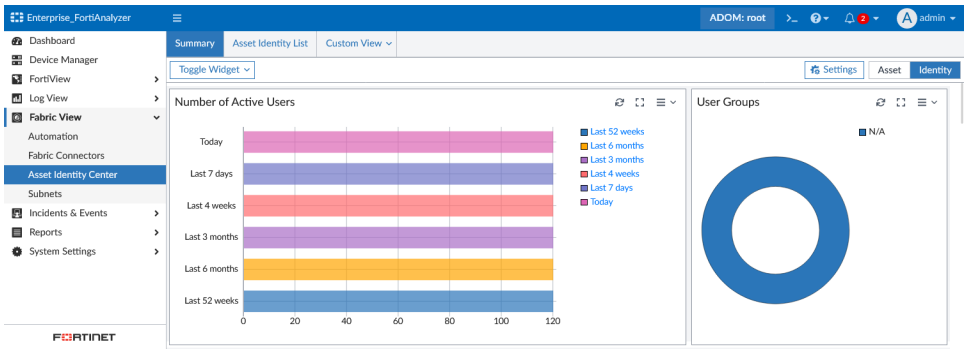
Go to *Fabric View* > *Asset Identity Center* > *Summary*. By default, the pane displays the *Asset* dashboard. You can click *Identity* to display the *Identity* dashboard. From the *Toggle Widgets* dropdown, select which widgets should display on the dashboard. You can filter all widgets on the dashboard from *Settings*.



The *Asset* dashboard includes the following widgets:

Detection Method	Displays endpoint detections by method.
Detection Source	Displays a breakdown of the asset center data sources.
Identification/Unidentified Asset	Displays the number of detected endpoint assets that are identified and unidentified.

Hardware/OS Distribution	Displays endpoint hardware operating system distribution.
Discovery Timeline	Displays an asset discovery timeline.
Identified Active Asset	Displays identified asset visibility over the past 24 hours to 52 weeks.
Assets By Location	Displays identified assets by location.
Identified Activity Timeline	Displays a first seen, last update, and last seen identified asset activity timeline.
Changes Timeline	Displays an asset changes timeline.
Unidentifed Active Asset	Displays unidentified asset visibility over the past 24 hours to 52 weeks.
Unidentifed Activity Timeline	Displays a first seen, last update, and last seen unidentified asset activity timeline.



The *Identity* dashboard includes the following widgets:

Top Users	Displays asset user data.
Number of Active Users	Displays user visibility data over the past 24 hours to 52 weeks.
User Groups	Displays user groups.
User's Location	Displays user numbers by location.
User's Manager	Displays user numbers by manager.
Discovery Timeline	Displays the user discovery timeline.
Activity Timeline	Displays the user activity timeline.
Endpoint Tag Distribution	Displays the distribution of endpoint tags.

Others

This section lists the new features added to FortiAnalyzer for other topics related to security operations:

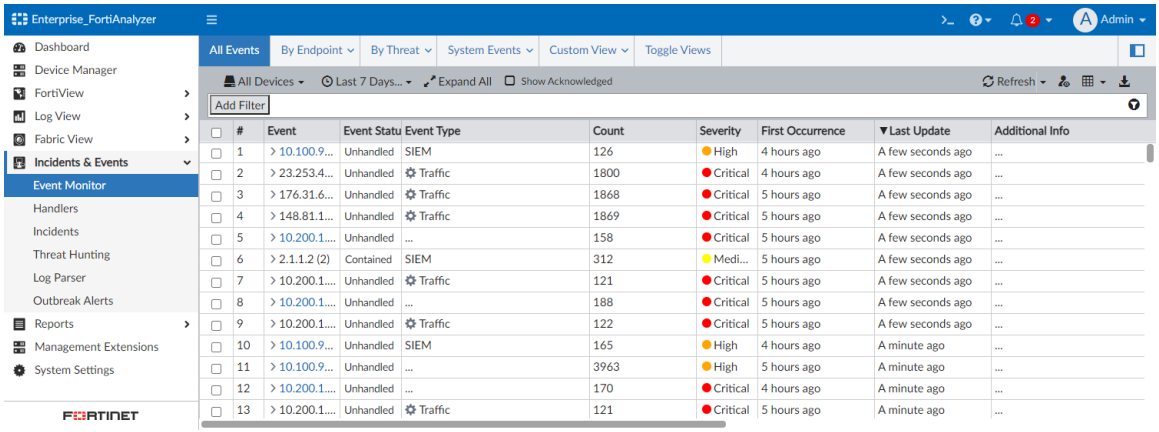
- FortiSoC GUI reorganization on page 11
- Notifications for new Outbreak Alerts 7.4.1 on page 14

FortiSoC GUI reorganization

The *FortiSoC* features have been organized in the following areas of the GUI:

- *Incidents & Events*
- *FortiView*
- *Fabric View*

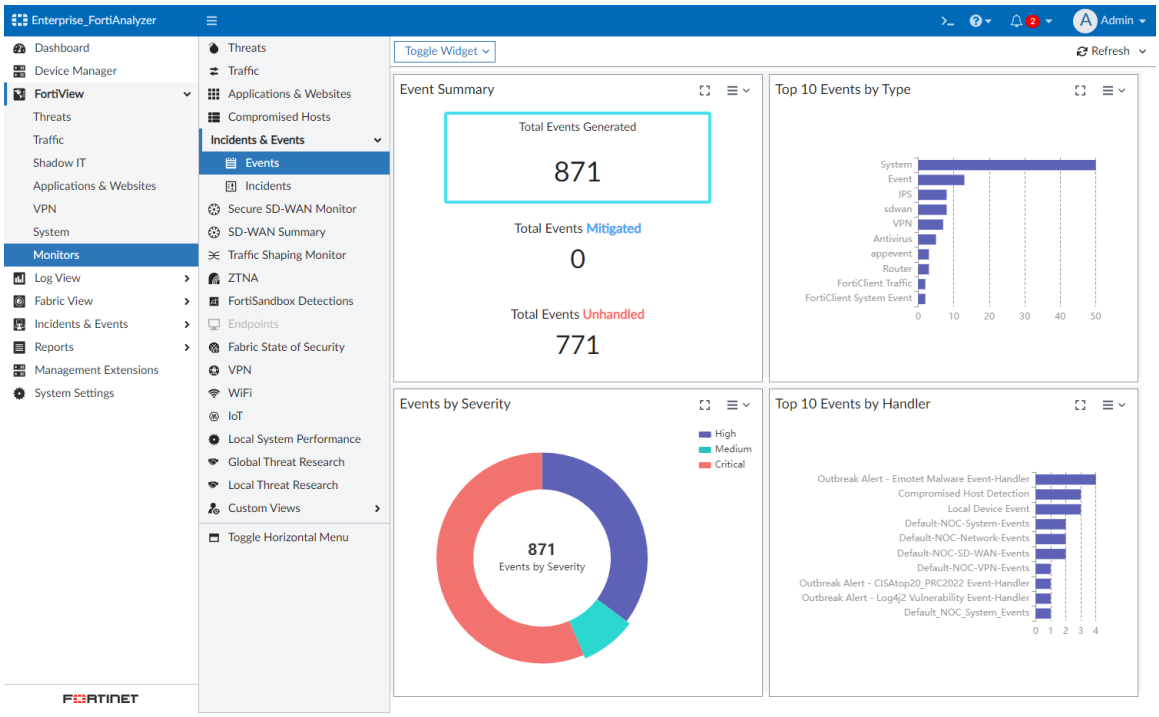
To create and manage events, go to *Incidents & Events*.

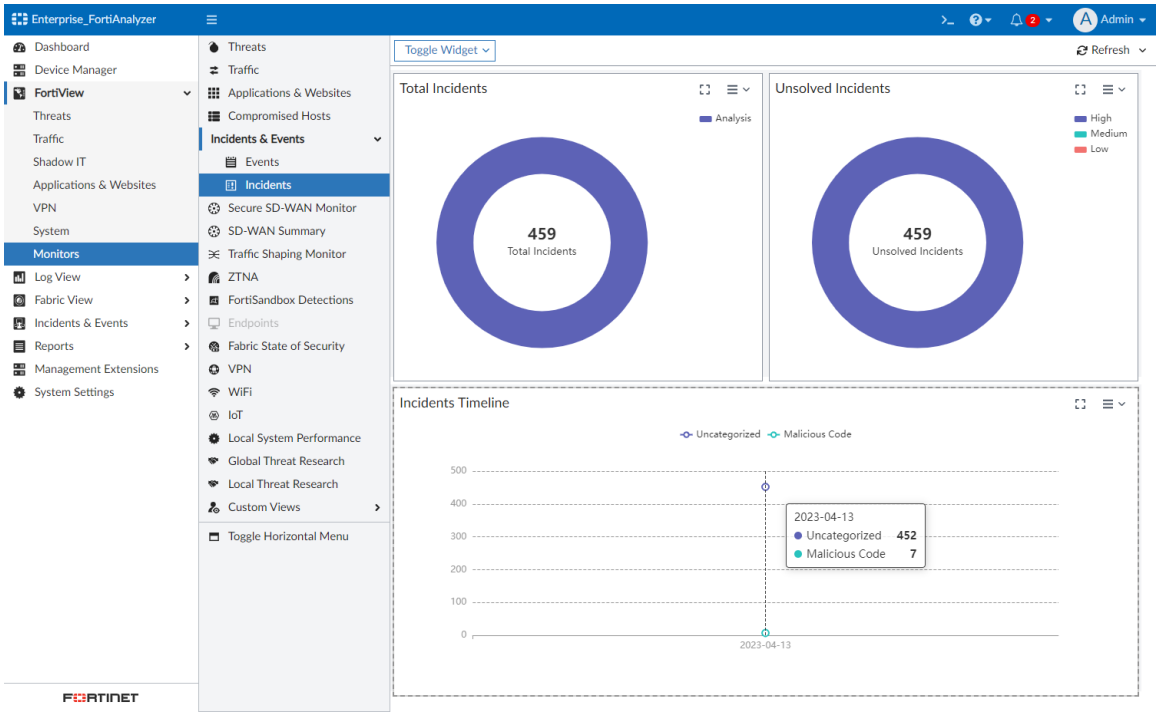


Incidents & Events includes the following:

Event Monitor	View events generated by event handlers. For more information, see the FortiAnalyzer Administration Guide.
Handlers	Configure data selectors, notification profiles, basic event handlers, and correlation event handlers. For more information, see the FortiAnalyzer Administration Guide.
Incidents	Create and update incidents to track and analyze events. For more information, see the FortiAnalyzer Administration Guide.
Threat Hunting	View a log count chart and SIEM log analytics table. The *Threat Hunting* dashboard is only available in Fabric ADOMs when ADOMs are enabled. For more information, see the FortiAnalyzer Administration Guide.
Log Parser	View and manage SIEM log parsers. For more information, see the FortiAnalyzer Administration Guide.
Outbreak Alerts	View outbreak alerts and automatically download related event handlers and reports from FortiGuard. The FortiAnalyzer Outbreak Detection Service is a licensed feature. For more information, see the FortiAnalyzer Administration Guide.

To review incidents and events in dashboards, go to *FortiView* > *Monitors* > *Incidents & Events*.



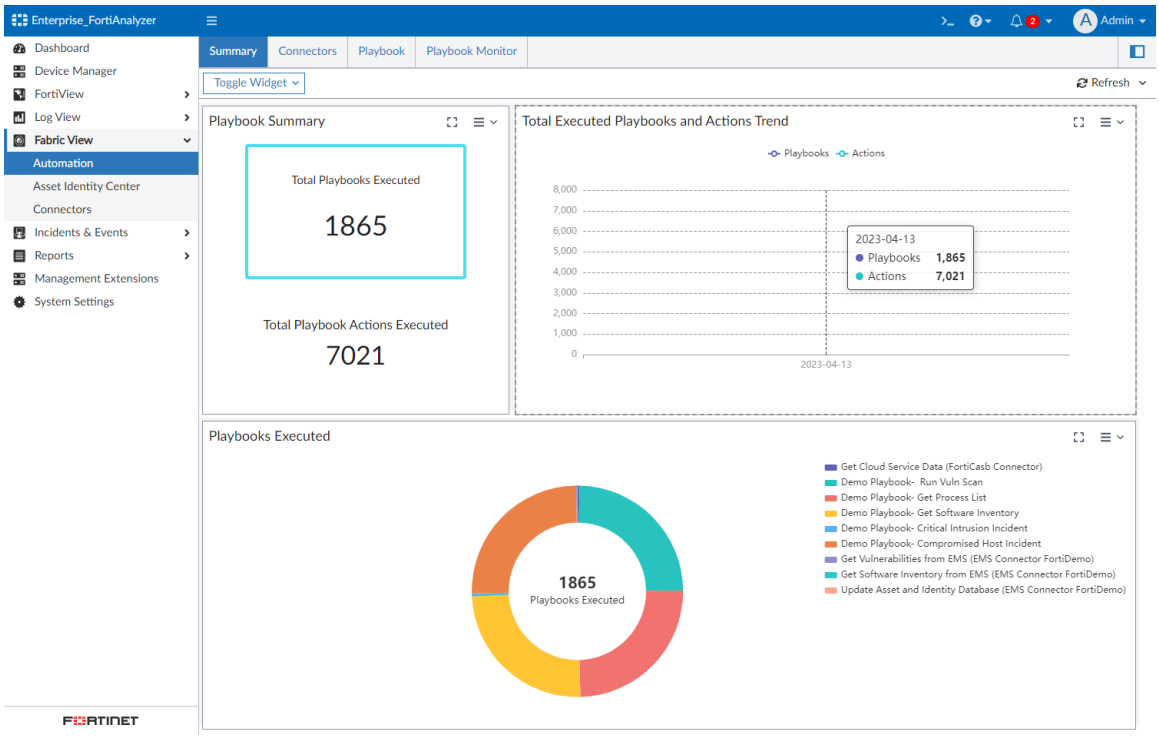


FortiView > *Monitors* > *Incidents & Events* includes the following dashboards:

Events	This dashboard includes the following widgets: • *Event Summary* • *Top 10 Events by Type* • *Events by Severity*

	• *Top 10 Events by Handler*
Incidents	This dashboard includes the following widgets: • *Total Incidents* • *Unsolved Incidents* • *Incidents Timeline*

To configure FortiSoC playbooks, go to *Fabric View* > *Automation*.



Fabric View > *Automation* includes the following:

Summary	View playbook performance in a dashboard. This includes widgets for total playbooks, playbooks executed, and an actions trend. For more information, see the FortiAnalyzer Administration Guide.
Connectors	View the status of available connectors supported for playbook automation. For more information, see the FortiAnalyzer Administration Guide.
Playbook	Configure and manage playbooks. For more information, see the FortiAnalyzer Administration Guide.
Playbook Monitor	View playbook jobs in a table view. For more information, see the FortiAnalyzer Administration Guide.

Notifications for new Outbreak Alerts - 7.4.1

This information is also available in the FortiAnalyzer 7.4 Administration Guide:

- Outbreak Alerts

When new Outbreak Alerts are received, GUI notifications are added in the banner, ensuring timely notification for administrators.

In the *Outbreak Alerts* pane, the Outbreak Alerts can now be sorted by *Date* or *Severity*, allowing for easy browsing and retrieval based on these criteria. A "*New*" tag is also added to alerts received in the current month to distinguish them from previous alerts.

For example, see the image below.

Use the tree menu in the sidebar to expand and browse the list of alerts.

After refreshing the pane, you will no longer see the *New* tag.

To group alerts in the sidebar by severity instead of *Date*, select the *Severity* radio button.

Log and Report

This section lists the new features added to FortiAnalyzer for logs and reports:

- Logging on page 16
- Log Forwarding on page 30
- Reports on page 34
- Others on page 46

Logging

This section lists the new features added to FortiAnalyzer for logging:

- FortiAnalyzer supports FortiWeb Cloud attack logs on page 16
- Support parsing and addition of third-party application logs to the SIEM DB on page 17
- Per-ADOM log rate on page 22
- Support EMS multitenancy via FortiAnalyzer ADOMs 7.4.1 on page 24
- Logging support for FortiCASB 7.4.1 on page 26
- Logging support for FortiPAM 7.4.1 on page 28
- Logging support for FortiToken Cloud 7.4.1 on page 29

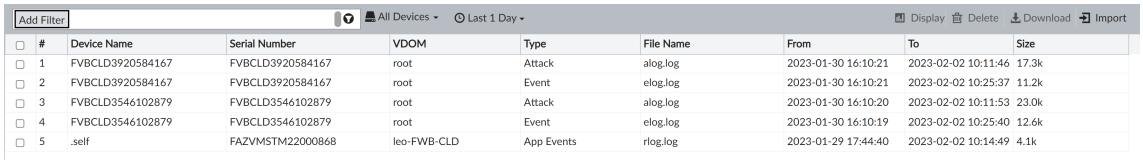
FortiAnalyzer supports FortiWeb Cloud attack logs

FortiAnalyzer now supports FortiWeb Cloud attack logs, and additional event/attack log fields have been added.

After adding and authorizing a FortiWeb Cloud device in FortiAnalyzer, you can view Attack and Event logs from this device in *Log View*.

To view FortiWeb Cloud logs in FortiAnalyzer:

1. In *Device Manager*, add and authorize the FortiWeb Cloud device.
2. To view logs from the FortiWeb Cloud device, go to *Log View* > *Log Browse*.

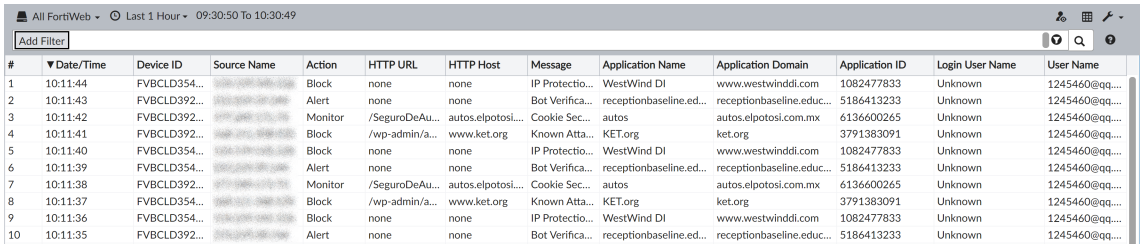


#	Device Name	Serial Number	VDOM	Type	File Name	From	To	Size
1	FVBCLD3920584167	FVBCLD3920584167	root	Attack	alog.log	2023-01-30 16:10:21	2023-02-02 10:11:46	17.3k
2	FVBCLD3920584167	FVBCLD3920584167	root	Event	elog.log	2023-01-30 16:10:21	2023-02-02 10:25:37	11.2k
3	FVBCLD3546102879	FVBCLD3546102879	root	Attack	alog.log	2023-01-30 16:10:20	2023-02-02 10:11:53	23.0k
4	FVBCLD3546102879	FVBCLD3546102879	root	Event	elog.log	2023-01-30 16:10:19	2023-02-02 10:25:40	12.6k
5	.self	FAZVMSTM22000868	leo-FWB-CLD	App Events	rlog.log	2023-01-29 17:44:40	2023-02-02 10:14:49	4.1k

You can also go to *Log View* > *FortiWeb* > *Attack*. This includes FortiWeb Cloud attack logs, as well as four new fields:

- *user_id*, which corresponds to the *User ID* column
- *app_id*, which corresponds to the *Application ID* column
- *app_name*, which corresponds to the *Application Name* column
- *app_domain*, which corresponds to the *Application Domain* column

See an example of *Log View* > *FortiWeb* > *Attack* below.

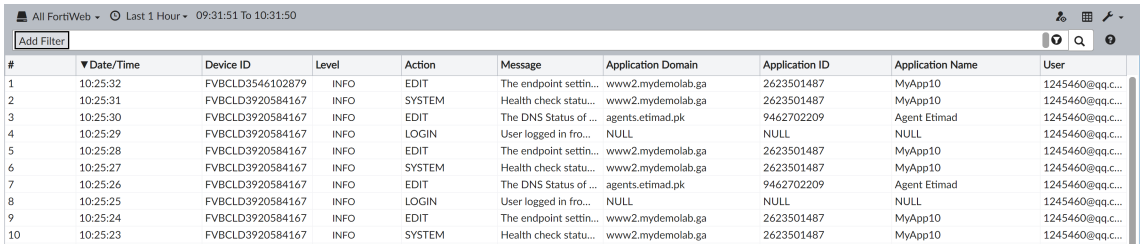


#	▼Date/Time	Device ID	Source Name	Action	HTTP URL	HTTP Host	Message	Application Name	Application Domain	Application ID	Login User Name	User Name
1	10:11:44	FVBCLD354...		Block	none	none	IP Protectio...	WestWind DI	www.westwinddi.com	1082477833	Unknown	1245460@qq....
2	10:11:43	FVBCLD392...		Alert	none	none	Bot Verifica...	receptionbaseline.ed...	receptionbaseline.educ...	5186413233	Unknown	1245460@qq....
3	10:11:42	FVBCLD392...		Monitor	/SeguroDeAu...	autos.elpotosi....	Cookie Sec...	autos	autos.elpotosi.com.mx	6136600265	Unknown	1245460@qq....
4	10:11:41	FVBCLD392...		Block	/wp-admin/a...	www.ket.org	Known Atta...	KET.org	ket.org	3791383091	Unknown	1245460@qq....
5	10:11:40	FVBCLD354...		Block	none	none	IP Protectio...	WestWind DI	www.westwinddi.com	1082477833	Unknown	1245460@qq....
6	10:11:39	FVBCLD354...		Alert	none	none	Bot Verifica...	receptionbaseline.ed...	receptionbaseline.educ...	5186413233	Unknown	1245460@qq....
7	10:11:38	FVBCLD392...		Monitor	/SeguroDeAu...	autos.elpotosi....	Cookie Sec...	autos	autos.elpotosi.com.mx	6136600265	Unknown	1245460@qq....
8	10:11:37	FVBCLD354...		Block	/wp-admin/a...	www.ket.org	Known Atta...	KET.org	ket.org	3791383091	Unknown	1245460@qq....
9	10:11:36	FVBCLD354...		Block	none	none	IP Protectio...	WestWind DI	www.westwinddi.com	1082477833	Unknown	1245460@qq....
10	10:11:35	FVBCLD392...		Alert	none	none	Bot Verifica...	receptionbaseline.ed...	receptionbaseline.educ...	5186413233	Unknown	1245460@qq....

Finally, you can also go to *Log View* > *FortiWeb* > *Event*. This includes FortiWeb Cloud event logs, as well as five new fields:

- *user_id*, which corresponds to the *User ID* column
- *login_user*, which corresponds to the *User* column
- *app_id*, which corresponds to the *Application ID* column
- *app_name*, which corresponds to the *Application Name* column
- *app_domain*, which corresponds to the *Application Domain* column

See an example of *Log View* > *FortiWeb* > *Event* below.



#	▼Date/Time	Device ID	Level	Action	Message	Application Domain	Application ID	Application Name	User
1	10:25:32	FVBCLD3546102879	INFO	EDIT	The endpoint settin...	www2.mydemolab.ga	2623501487	MyApp10	1245460@qq.c...
2	10:25:31	FVBCLD3920584167	INFO	SYSTEM	Health check statu...	www2.mydemolab.ga	2623501487	MyApp10	1245460@qq.c...
3	10:25:30	FVBCLD3920584167	INFO	EDIT	The DNS Status of ...	agents.etimad.pk	9462702209	Agent Etimad	1245460@qq.c...
4	10:25:29	FVBCLD3920584167	INFO	LOGIN	User logged in fro...	NULL	NULL	NULL	1245460@qq.c...
5	10:25:28	FVBCLD3920584167	INFO	EDIT	The endpoint settin...	www2.mydemolab.ga	2623501487	MyApp10	1245460@qq.c...
6	10:25:27	FVBCLD3920584167	INFO	SYSTEM	Health check statu...	www2.mydemolab.ga	2623501487	MyApp10	1245460@qq.c...
7	10:25:26	FVBCLD3920584167	INFO	EDIT	The DNS Status of ...	agents.etimad.pk	9462702209	Agent Etimad	1245460@qq.c...
8	10:25:25	FVBCLD3920584167	INFO	LOGIN	User logged in fro...	NULL	NULL	NULL	1245460@qq.c...
9	10:25:24	FVBCLD3920584167	INFO	EDIT	The endpoint settin...	www2.mydemolab.ga	2623501487	MyApp10	1245460@qq.c...
10	10:25:23	FVBCLD3920584167	INFO	SYSTEM	Health check statu...	www2.mydemolab.ga	2623501487	MyApp10	1245460@qq.c...

Support parsing and addition of third-party application logs to the SIEM DB

This information is also available in the FortiAnalyzer 7.4 Administration Guide:

- SIEM log parsers

FortiAnalyzer supports parsing and addition of third-party application logs to the SIEM DB.

There are two types of log parsers:

- Predefined parsers
- Custom parsers

You can find predefined SIEM log parsers in *Incidents & Events* > *Log Parser* > *Log Parsers*. There are predefined parsers for all fabric related Fortinet products. Predefined Apache and Nginx web server log parsers have also been added to this list of predefined SIEM log parsers.

The configuration of each SIEM log parser (predefined and custom) is specific to the ADOM that you are in. Any changes to an existing parser or any newly added parsers will only affect the ADOM that the action was completed in. Ensure you are in the correct ADOM when working with log parsers.

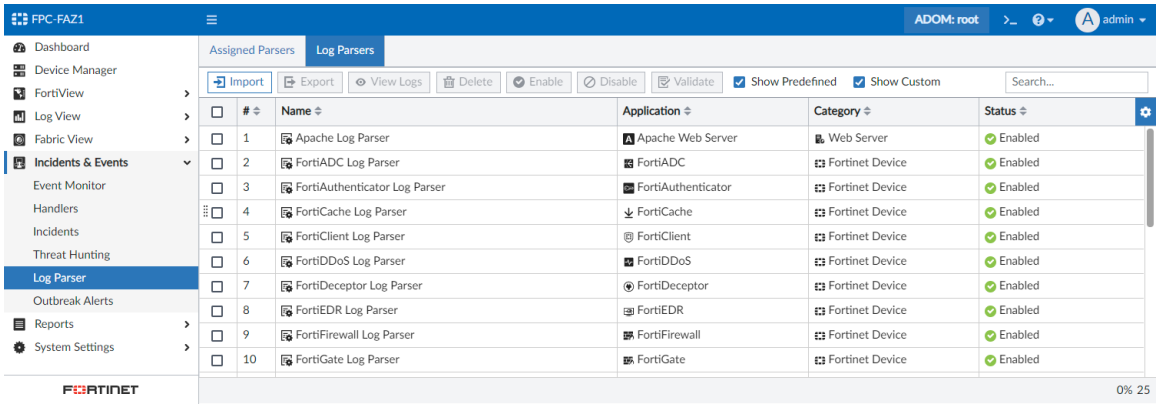
The following information is provided in this topic:

- To view the log parsers: on page 18
- The Apache web server log parser: on page 19

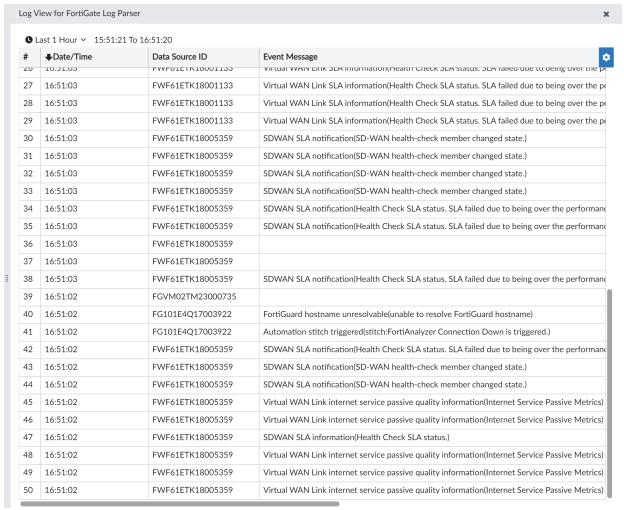
- The Nginx web server log parser: on page 19
- To import a custom log parser: on page 20
- To validate if the original logs can be parsed: on page 21
- To assign devices to a log parser: on page 21

To view the log parsers:

1. In *Incidents & Events* > *Log Parser* > *Log Parsers*, select *Show Predefined* and/or *Show Custom* to show the available log parsers in the table view.
   Each predefined log parser is assigned a default *Application* and *Category*. Custom log parsers are assigned a default *Application* and *Category* when they are imported.
   The # column is the priority of each Siem Log_Parser from highest (1) to lowest. By default, newly imported custom log parsers are assigned the lowest priority. To change the priority, click the left edge of the row and drag and drop it to the desired area in the table. See below.

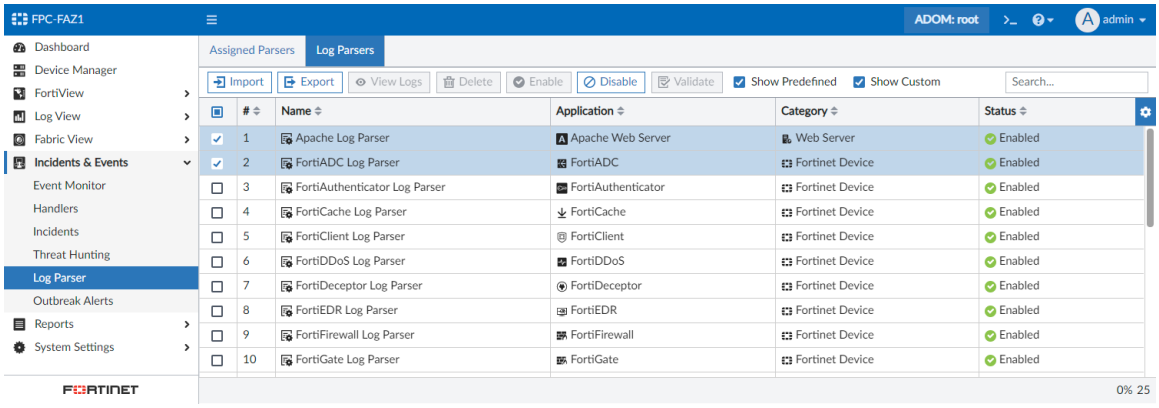


2. Double-click a log parser in the table view to display all related SIEM logs. Alternatively, you can select the checkbox for the log parser and click *View Logs*.



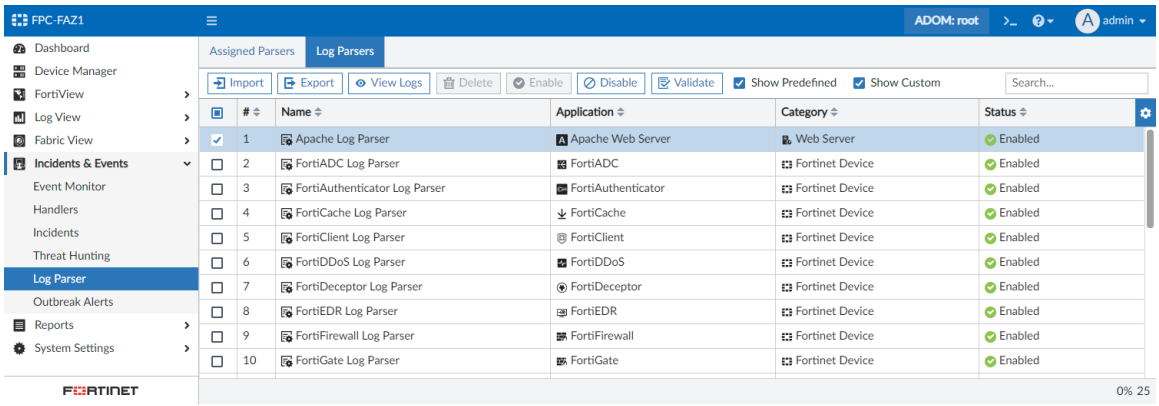
3. Select the checkbox for one or more log parsers in the table to perform an action from the toolbar.
   For example, you can *Export* in JSON format, *Enable*, *Disable*, *Delete*, or *Validate* the log parsers.
   Some actions will be unavailable if they cannot be performed on the selected log parser(s).
   - You cannot *Disable* a log parser if it is assigned and in use.
   - You cannot *Delete* predefined log parsers. They can only be disabled.

- You cannot perform the *Validate* action on more than one parser at a time.

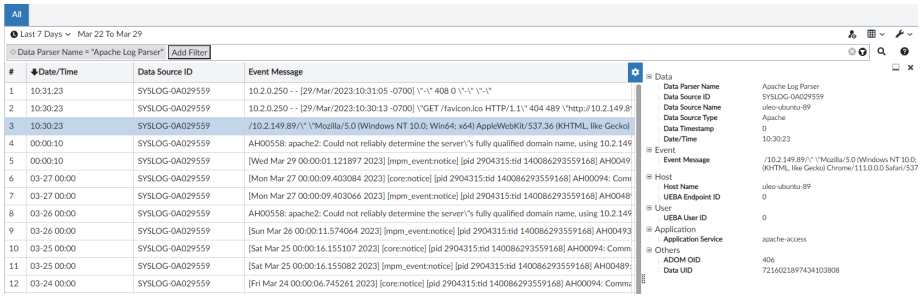


The Apache web server log parser:

Go to *Incidents & Events* > *Log Parser* > *Log Parsers* to find the Apache Log Parser in the predefined SIEM log parsers. Double-click the parser to view the related logs.

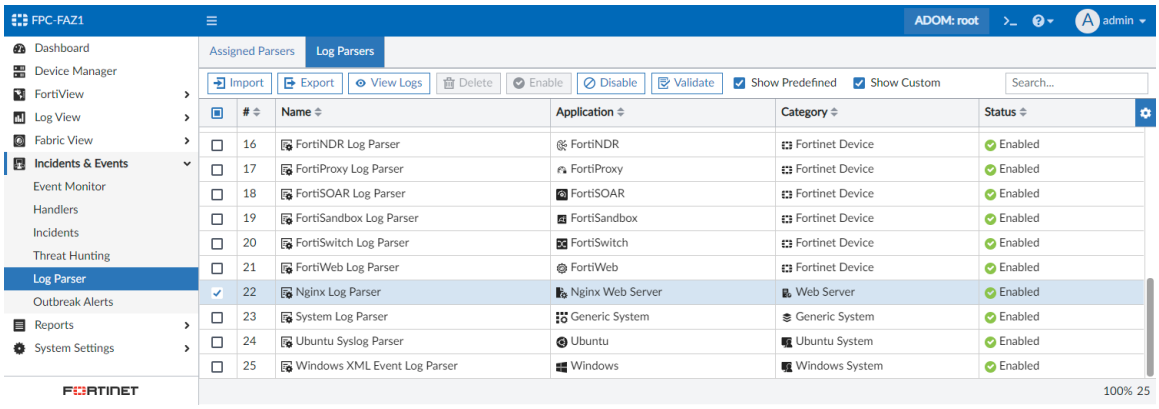


The Apache logs are also parsed in *Log View* > *Fabric* > *All*. You can filter by `Data Parser Name = Apache Log Parser`.

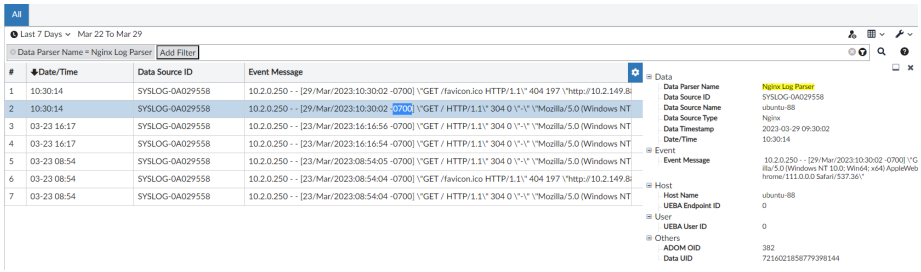


The Nginx web server log parser:

Go to *Incidents & Events* > *Log Parser* > *Log Parsers* to find the Nginx Log Parser in the predefined SIEM log parsers. Double-click the parser to view the related logs.

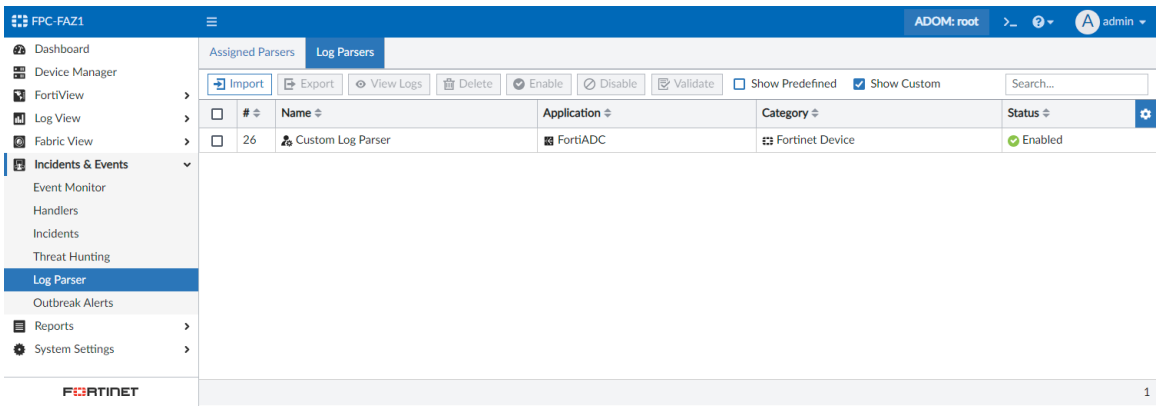


The Nginx logs are also parsed in *Log View* > *Fabric* > *All*. You can filter by `Data Parser Name = Nginx Log Parser`.



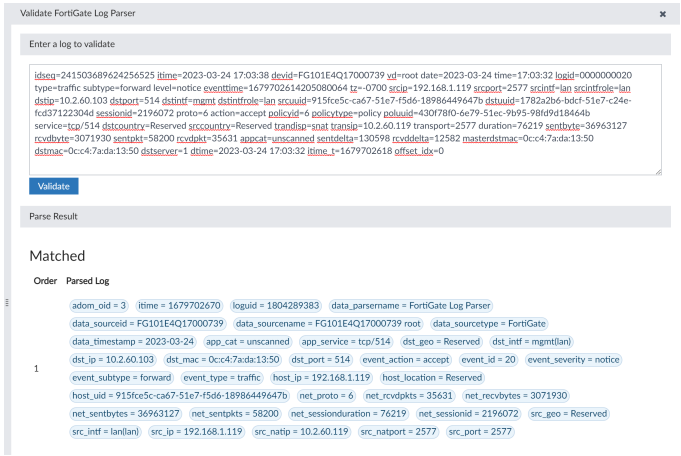
To import a custom log parser:

1. In *Incidents & Events* > *Log Parser* > *Log Parsers*, click *Import*.
   The *Import Log Parser* dialog displays.
2. Drag and drop or select the log parser.
   The log parser must be in the correct format as a JSON file to meet the requirements checked during the import.
3. Click *OK*.
   Once added, the custom log parser will be included in the table view when *Show Custom* is selected.



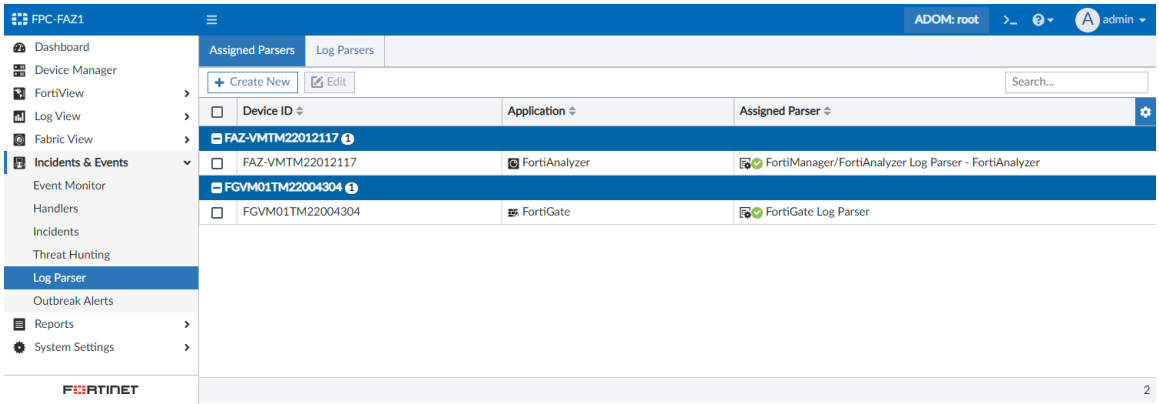
To validate if the original logs can be parsed:

1. In *Incidents & Events* > *Log Parser* > *Log Parsers*, select the checkbox for a log parser.
2. Click *Validate*.
   The *Validate Log Parser* pane opens.
3. Enter a log to validate and click *Validate*.
   A *Parse Result* will display in the same pane.



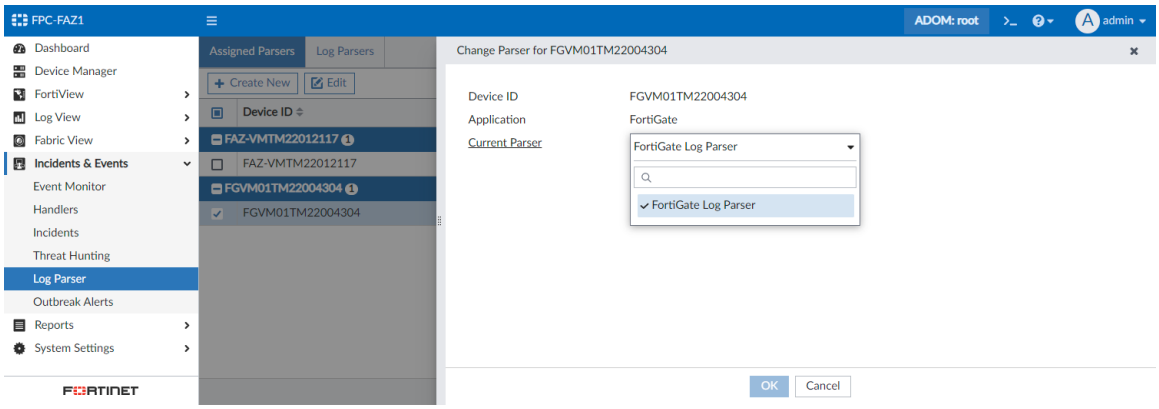
To assign devices to a log parser:

1. Go to *Incidents & Events* > *Log Parser* > *Assigned Parsers*.
   The existing log parser assignments display in a table view.



2. Select the checkbox for an existing log parser assignment and click *Edit*.
   Alternatively, you can click *Create New* to create a new log parser assignment.
   The *Change Parser* pane displays.
3. From the *Current Parser* dropdown, select the log parser to assign the device/application to.

4. Click *OK*.



Per-ADOM log rate

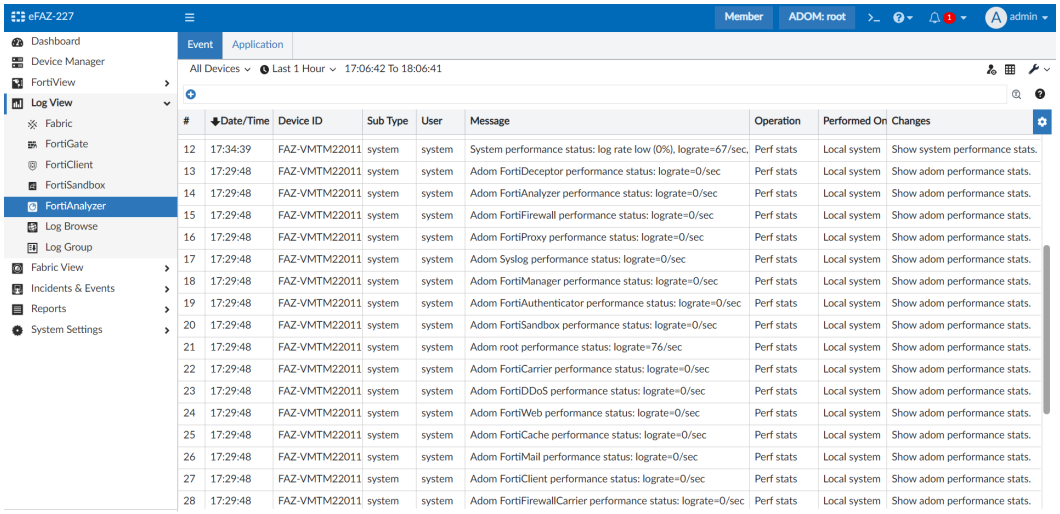
To better fit multi-tenancy deployment, FortiAnalyzer provides a per-ADOM log rate that the administrator can monitor to prevent one ADOM/customer from impacting the stability of the entire unit.

An additional diskquota log has been introduced to inform the administrator when an ADOM reaches the configured quota threshold.

To view the logs in the GUI:

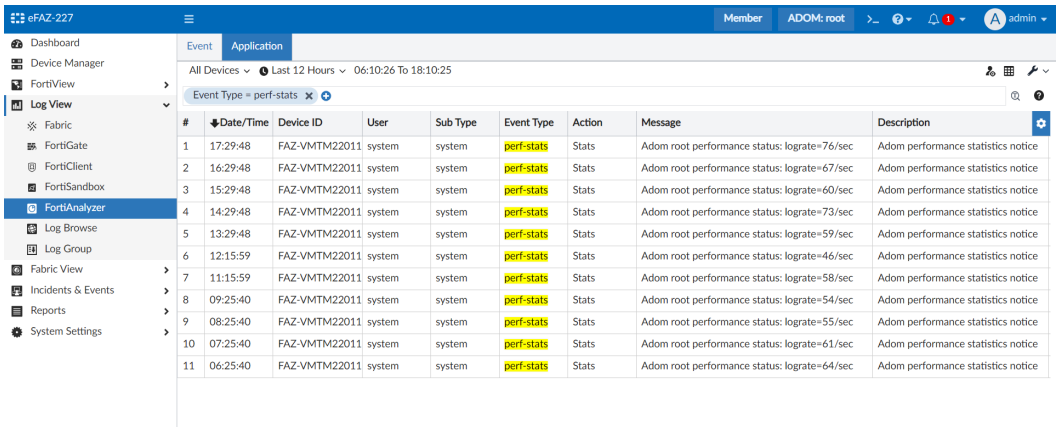
A log message for ADOM performance statistics (log rate) is added to both FortiAnalyzer Event logs and Application logs. FortiAnalyzer Event logs will generate this message for all ADOMs, while Application logs will generate this message for the current ADOM only.

For example, see the below log messages in *Log View* > *FortiAnalyzer* > *Event*:



#	Date/Time	Device ID	Sub Type	User	Message	Operation	Performed On	Changes
12	17:34:39	FAZ-VMTM22011	system	system	System performance status: log rate low (0%), lograte=67/sec,	Perf stats	Local system	Show system performance stats.
13	17:29:48	FAZ-VMTM22011	system	system	Adom FortiDeceptor performance status: lograte=0/sec	Perf stats	Local system	Show adom performance stats.
14	17:29:48	FAZ-VMTM22011	system	system	Adom FortiAnalyzer performance status: lograte=0/sec	Perf stats	Local system	Show adom performance stats.
15	17:29:48	FAZ-VMTM22011	system	system	Adom FortiFirewall performance status: lograte=0/sec	Perf stats	Local system	Show adom performance stats.
16	17:29:48	FAZ-VMTM22011	system	system	Adom FortiProxy performance status: lograte=0/sec	Perf stats	Local system	Show adom performance stats.
17	17:29:48	FAZ-VMTM22011	system	system	Adom Syslog performance status: lograte=0/sec	Perf stats	Local system	Show adom performance stats.
18	17:29:48	FAZ-VMTM22011	system	system	Adom FortiManager performance status: lograte=0/sec	Perf stats	Local system	Show adom performance stats.
19	17:29:48	FAZ-VMTM22011	system	system	Adom FortiAuthenticator performance status: lograte=0/sec	Perf stats	Local system	Show adom performance stats.
20	17:29:48	FAZ-VMTM22011	system	system	Adom FortiSandbox performance status: lograte=0/sec	Perf stats	Local system	Show adom performance stats.
21	17:29:48	FAZ-VMTM22011	system	system	Adom root performance status: lograte=76/sec	Perf stats	Local system	Show adom performance stats.
22	17:29:48	FAZ-VMTM22011	system	system	Adom FortiCarrier performance status: lograte=0/sec	Perf stats	Local system	Show adom performance stats.
23	17:29:48	FAZ-VMTM22011	system	system	Adom FortiDDoS performance status: lograte=0/sec	Perf stats	Local system	Show adom performance stats.
24	17:29:48	FAZ-VMTM22011	system	system	Adom FortiWeb performance status: lograte=0/sec	Perf stats	Local system	Show adom performance stats.
25	17:29:48	FAZ-VMTM22011	system	system	Adom FortiCache performance status: lograte=0/sec	Perf stats	Local system	Show adom performance stats.
26	17:29:48	FAZ-VMTM22011	system	system	Adom FortiMail performance status: lograte=0/sec	Perf stats	Local system	Show adom performance stats.
27	17:29:48	FAZ-VMTM22011	system	system	Adom FortiClient performance status: lograte=0/sec	Perf stats	Local system	Show adom performance stats.
28	17:29:48	FAZ-VMTM22011	system	system	Adom FortiFirewallCarrier performance status: lograte=0/sec	Perf stats	Local system	Show adom performance stats.

For example, see the below log messages in *Log View* > *FortiAnalyzer* > *Application*:



#	Date/Time	Device ID	User	Sub Type	Event Type	Action	Message	Description
1	17:29:48	FAZ-VMTM22011	system	system	perf-stats	Stats	Adom root performance status: lograte=76/sec	Adom performance statistics notice
2	16:29:48	FAZ-VMTM22011	system	system	perf-stats	Stats	Adom root performance status: lograte=67/sec	Adom performance statistics notice
3	15:29:48	FAZ-VMTM22011	system	system	perf-stats	Stats	Adom root performance status: lograte=60/sec	Adom performance statistics notice
4	14:29:48	FAZ-VMTM22011	system	system	perf-stats	Stats	Adom root performance status: lograte=73/sec	Adom performance statistics notice
5	13:29:48	FAZ-VMTM22011	system	system	perf-stats	Stats	Adom root performance status: lograte=59/sec	Adom performance statistics notice
6	12:15:59	FAZ-VMTM22011	system	system	perf-stats	Stats	Adom root performance status: lograte=46/sec	Adom performance statistics notice
7	11:15:59	FAZ-VMTM22011	system	system	perf-stats	Stats	Adom root performance status: lograte=58/sec	Adom performance statistics notice
8	09:25:40	FAZ-VMTM22011	system	system	perf-stats	Stats	Adom root performance status: lograte=54/sec	Adom performance statistics notice
9	08:25:40	FAZ-VMTM22011	system	system	perf-stats	Stats	Adom root performance status: lograte=55/sec	Adom performance statistics notice
10	07:25:40	FAZ-VMTM22011	system	system	perf-stats	Stats	Adom root performance status: lograte=61/sec	Adom performance statistics notice
11	06:25:40	FAZ-VMTM22011	system	system	perf-stats	Stats	Adom root performance status: lograte=64/sec	Adom performance statistics notice

A log message is also added for ADOM archive usage to Local Application Logs. See below example taken from *Log View* > *FortiAnalyzer* > *Application*:

#	Date/Time	Device ID	Sub Type	User	Message	Event Type	Description
1	2023-03-21 20:37:29	FAZ-VMTM23003736	diskquota	system	Disk usage for Adom Lab is approaching the delete threshold 90% of total 50.	disk-usage	Disk quota warning
2	2023-03-21 20:36:48	FAZ-VMTM23003736	system	system	Adom Lab performance status: log rate low (0%), lograte=1056/sec	perf-stats	Adom performance s
3	2023-03-21 20:31:48	FAZ-VMTM23003736	system	system	Adom Lab performance status: log rate low (0%), lograte=59/sec	perf-stats	Adom performance s
4	2023-03-21 20:31:40	FAZ-VMTM23003736	logdev	system	Did not receive any log from device eFGT-HA_FGVULV[FGVULVTM2100009	logging-status	Device offline
5	2023-03-21 20:23:56	FAZ-VMTM23003736	system	system	Adom Lab performance status: log rate low (0%), lograte=57/sec	perf-stats	Adom performance s
6	2023-03-21 20:18:56	FAZ-VMTM23003736	system	system	Adom Lab performance status: log rate low (0%), lograte=56/sec	perf-stats	Adom performance s
7	2023-03-21 20:13:56	FAZ-VMTM23003736	system	system	Adom Lab performance status: log rate low (0%), lograte=56/sec	perf-stats	Adom performance s
8	2023-03-21 20:08:56	FAZ-VMTM23003736	system	system	Adom Lab performance status: log rate low (0%), lograte=58/sec	perf-stats	Adom performance s
9	2023-03-21 20:03:56	FAZ-VMTM23003736	system	system	Adom Lab performance status: log rate low (0%), lograte=57/sec	perf-stats	Adom performance s
10	2023-03-21 19:58:56	FAZ-VMTM23003736	system	system	Adom Lab performance status: log rate low (0%), lograte=52/sec	perf-stats	Adom performance s
11	2023-03-21 19:58:47	FAZ-VMTM23003736	logdev	system	Did not receive any log from device eFGT-HA_FGVULV[FGVULVTM2100009	logging-status	Device offline

To set the interval for the ADOM performance statistics logs:

CLI configuration is added for the interval time to log performance state.

In the FortiAnalyzer CLI, enter the following command:

```
config system locallog setting
   set log-interval-adom-perf-stats <integer>
end
```

For the `log-interval-adom-perf-stats` setting, enter the interval in minutes. The range should be `5-2880`. Enter `0` to disable the logs.

Example logs:

Event log message for ADOM performance statistics (log rate):

```
id=7231962960615178247 bid=865533 dvid=1040 itime=1683822591 euid=1 epid=1 dsteuid=1
     dstepid=1 log_id="0001010093" subtype="system" type="event" level="notice"
     time="09:29:51" date="2023-05-11" user="system" action="Stats" msg="Adom root
     performance status: lograte=54/sec" userfrom="system" desc="Adom performance
     statistics notice" operation="Perf stats" performed_on="Local system" changes="Show
     adom performance stats." lograte=54 logratelimit=0 tz="-0700" devid="FAZ-VMTM22011553"
     devname="eFAZ-227"
```

Application log message for ADOM performance statistics (log rate):

```
id=7207521362594958664 bid=101707 dvid=1059 itime=1678131838 euid=1 epid=1 dsteuid=1
     dstepid=1 vd="fortinet" logid="220004" type="appevent" subtype="system"
     eventtype="perf-stats" action="Stats" level="notice" date="2023-03-06" time="11:43:58"
     user="system" user_from="system" desc="Adom performance statistics notice" msg="Adom
```

```
fortinet performance status: log rate low (0%), lograte=49/sec" tz="-0800"
adom="fortinet" operation="Perf stats" lograte=49 performed_on="Local system"
changes="Show adom performance stats." logratelimit=0 devid="FAZ-VMTM23003360"
devname="eFAZ-54"
```

Log message for ADOM archive usage:

```
id=7207519107737128256 bid=100933 dvid=1059 itime=1678131313 euid=1 epid=1 dsteuid=1
dstepid=1 vd="fortinet" logid="220003" type="appevent" subtype="diskquota"
eventtype="disk-usage" level="warning" date="2023-03-06" time="11:35:14" user="system"
user_from="system" desc="Disk quota warning" msg="Disk usage for Adom fortinet is
approaching the delete threshold 90% of total 50.0MB.  Archive Usage at 196.7%(29.5MB)
and Analytics Usage at 41.6%(14.6MB)." tz="-0800" adom="fortinet" diskusage=88
devid="FAZ-VMTM23003360" devname="eFAZ-54"
```

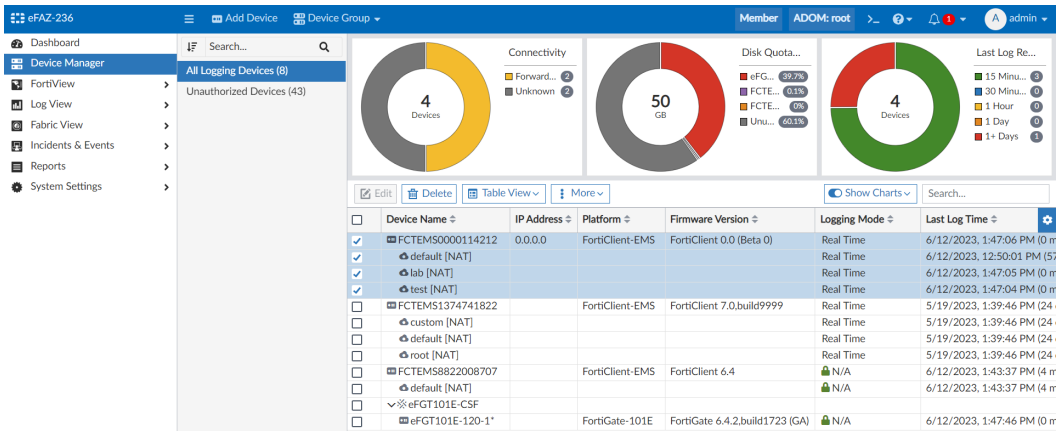
Support EMS multitenancy via FortiAnalyzer ADOMs - 7.4.1

With FortiClient EMS multitenancy, you can create multiple sites, providing granular access to different sites and separating endpoint data and configurations.

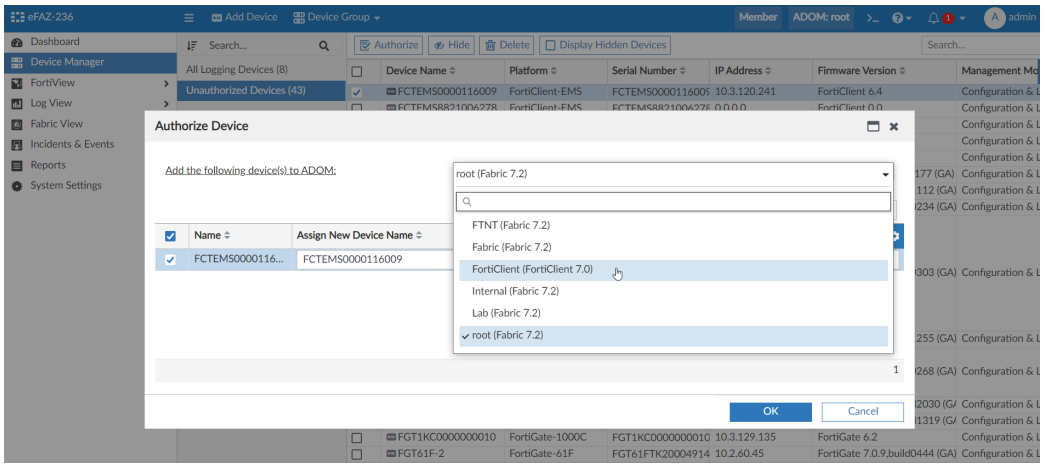
FortiAnalyzer has added support to EMS multitenancy by providing the following:

- Each log is mapped to its corresponding site using the `vd` log field
- EMS sites can be assigned to different FortiAnalyzer ADOMs

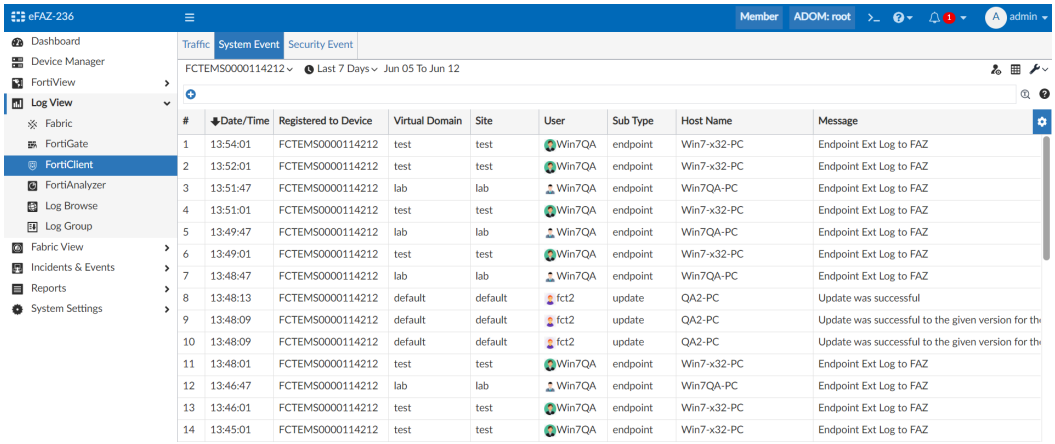
EMS logs (with multiple FCT logs) can be received by FortiAnalyzer directly with required fields added.



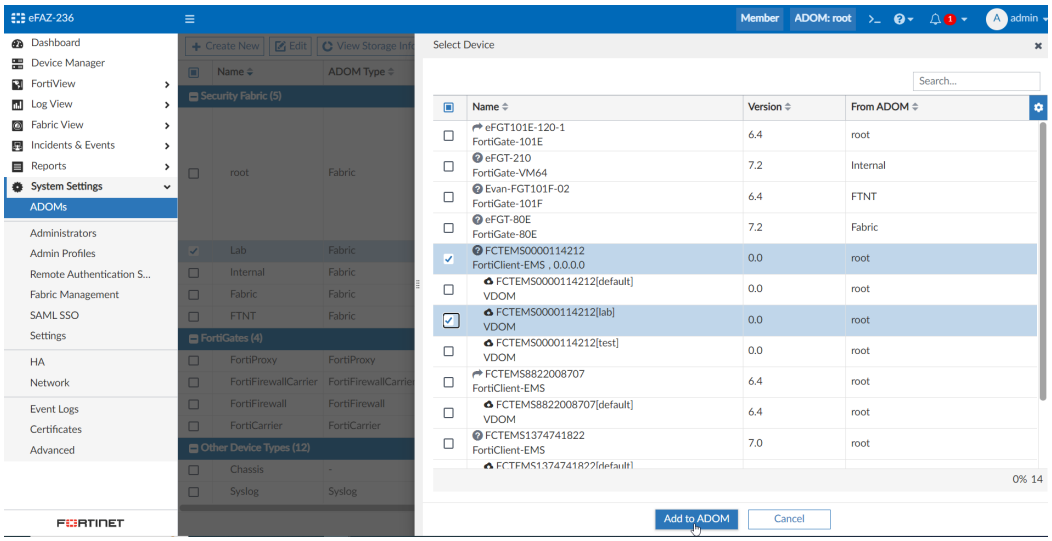
FortiClient can be promoted into Fabric ADOM or FortiClient ADOM in FortiAnalyzer.



The FortiClient logs from multitenancy logs can be converted to `vd=sitename` when receiving logs.



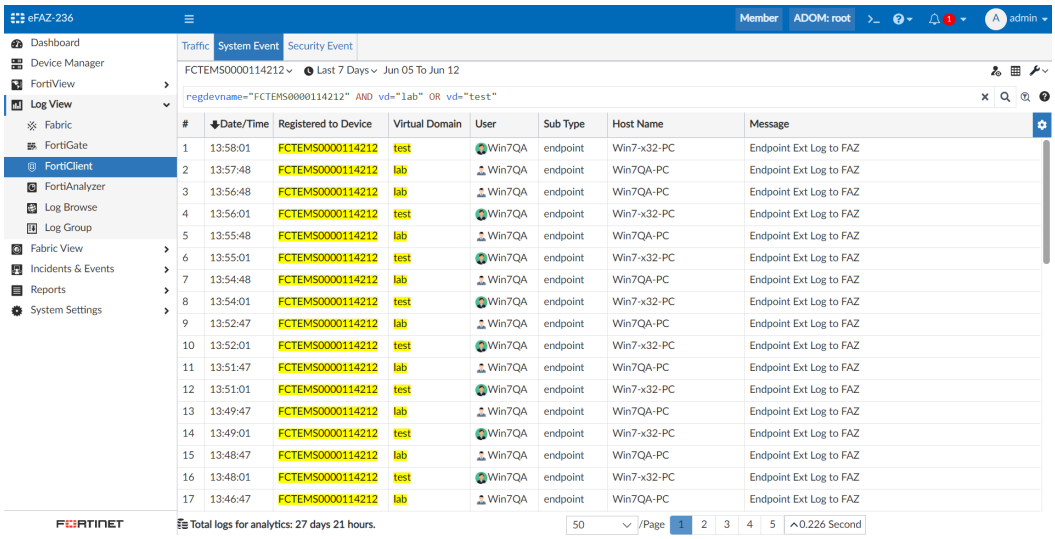
The multitenancy logs can be assigned to different ADOMs based on its VDOM when the *ADOM Mode* is set to *Advanced*.



Two new fields are added to FortiClient logs:

- `vd`
- `regdevname`

The FortiClient logs can be filtered by these fields in *Log View*. For example, see below.

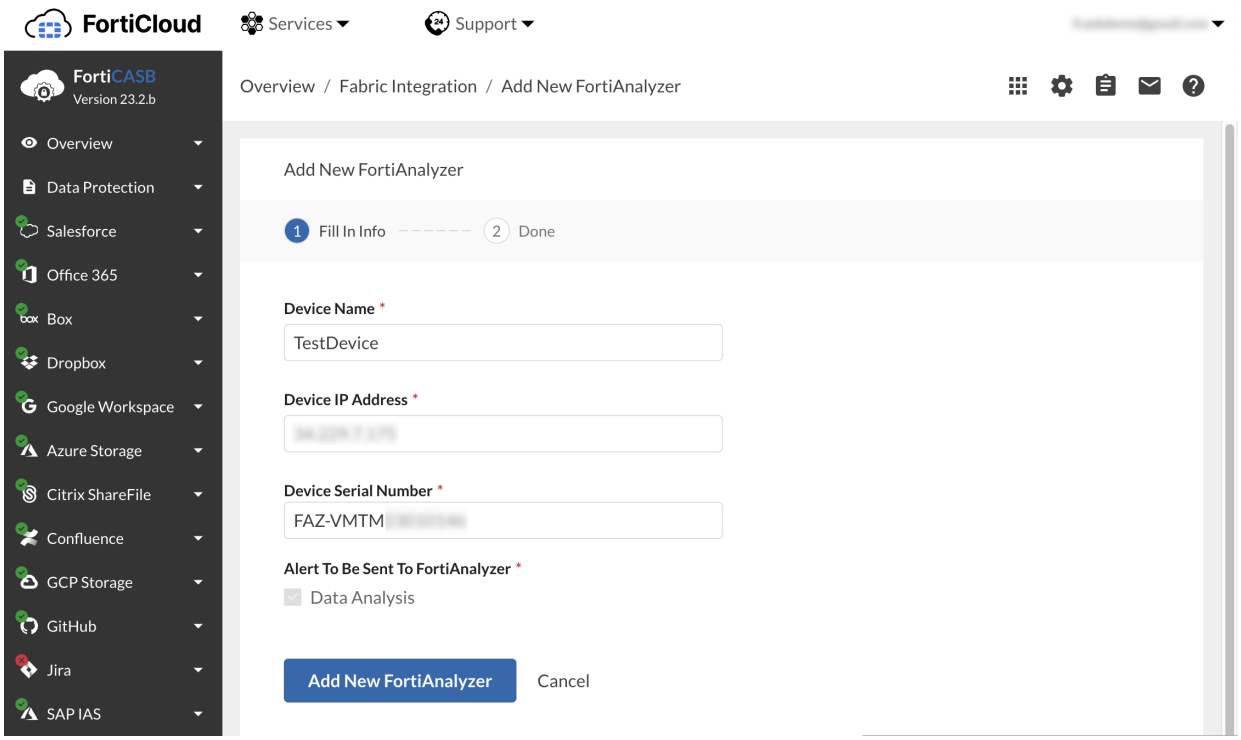


Logging support for FortiCASB - 7.4.1

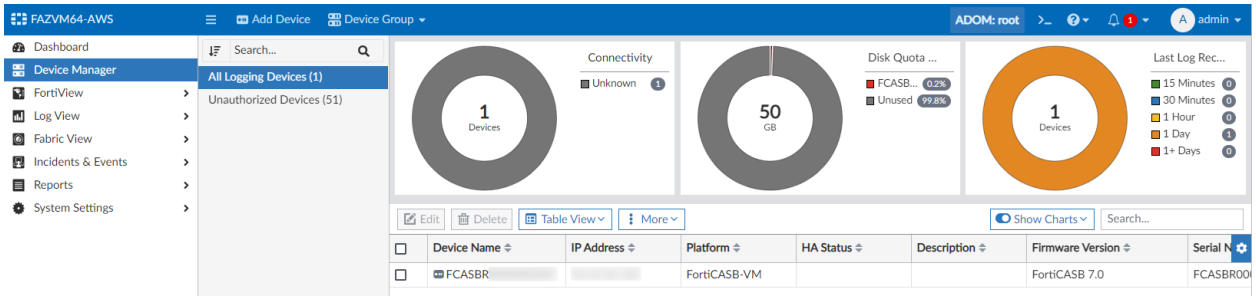
FortiAnalyzer can now receive, store, and display logs from authorized FortiCASB devices in *Log View*.

To configure FortiCASB logging to FortiAnalyzer:

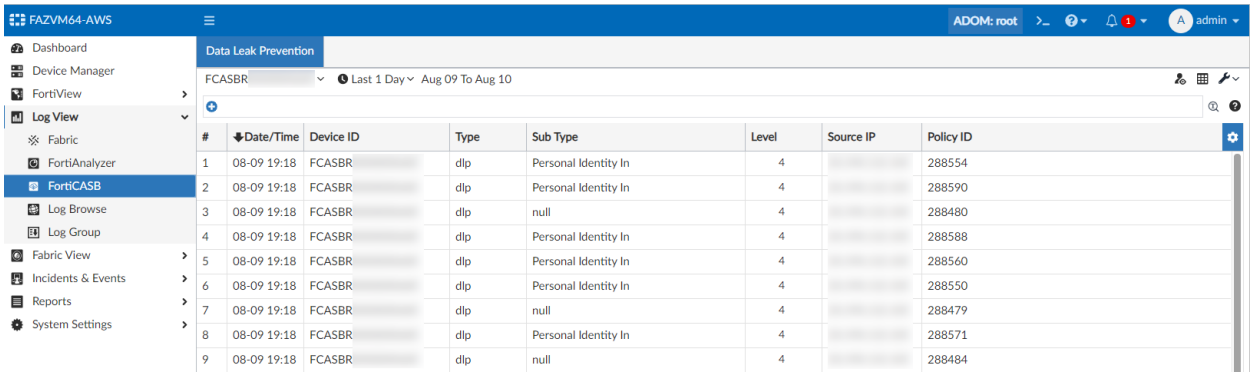
1. In the FortiCASB GUI, go to *Overview* > *Fabric Integration* > *Add New FortiAnalyzer*.
2. Configure the following settings for the FortiAnalyzer device and click *Add New FortiAnalyzer*:
   - *Device Name*
   - *Device IP Address*
   - *Device Serial Number*



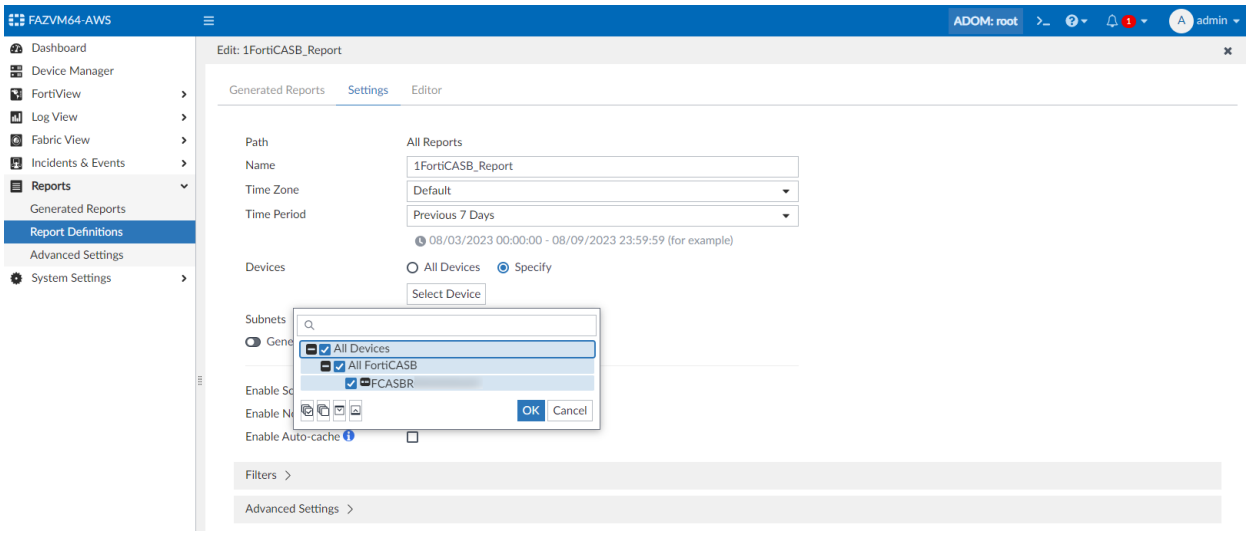
3. In the FortiAnalyzer GUI, go to *Device Manager* in the root ADOM.
   The FortiCASB displays in the *Unauthorized Devices* list.
4. Select the FortiCASB device and click *Authorize*.
   The FortiCASB device now displays in *All Logging Devices* list.



The FortiCASB logs display in *Log View* > *FortiCASB*.



The FortiCASB device can now be used in *Reports*.

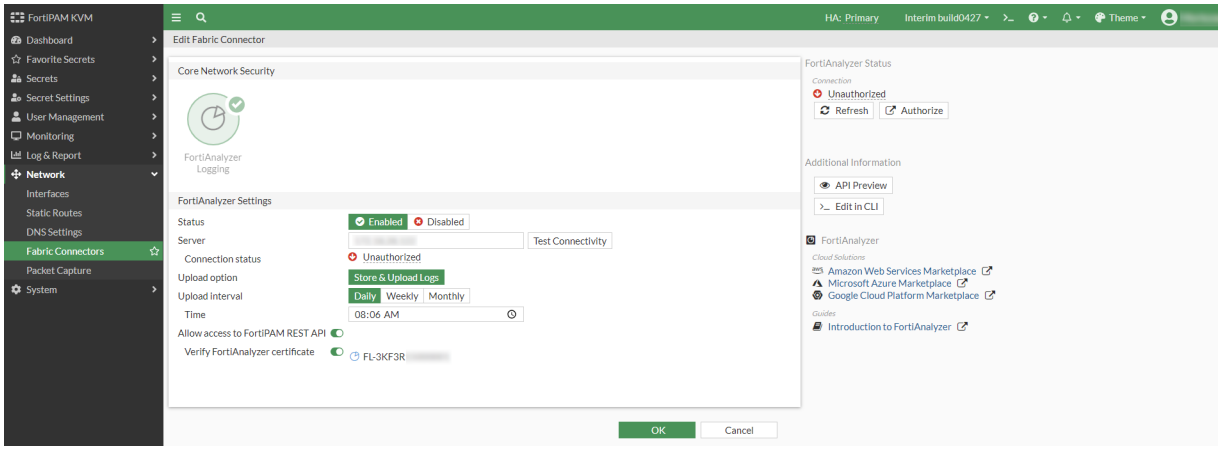


Logging support for FortiPAM - 7.4.1

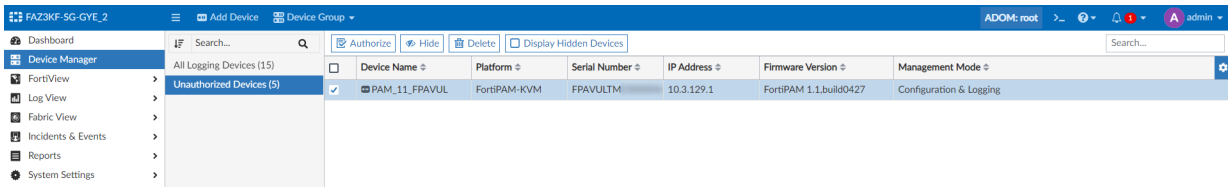
FortiAnalyzer now supports logs from FortiPAM.

To configure FortiPAM logging to FortiAnalyzer:

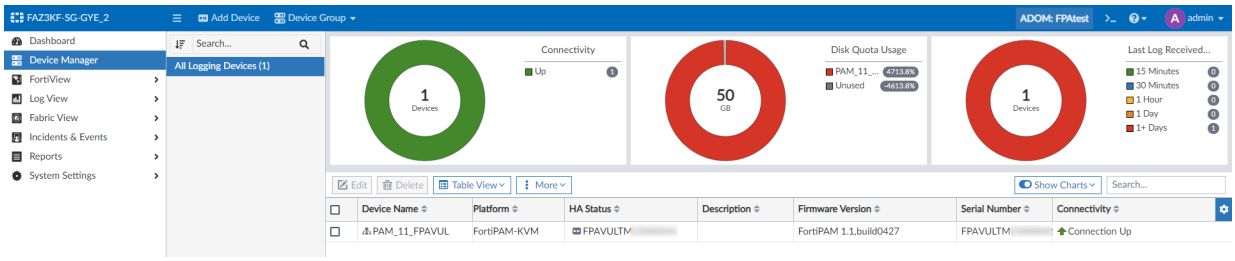
1. In the FortiPAM GUI, go to *Network* > *Fabric Connectors*, and edit *FortiAnalyzer Logging*. In the *Server* field, enter the FortiAnalyzer IP address.



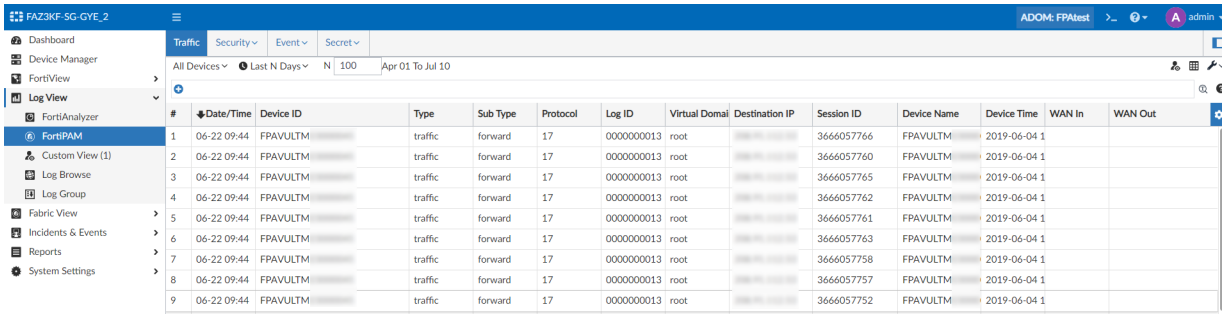
2. In the FortiAnalyzer GUI root ADOM, go to *Device Manager* > *Unauthorized Devices*. Select the FortiPAM device and click *Authorize*.



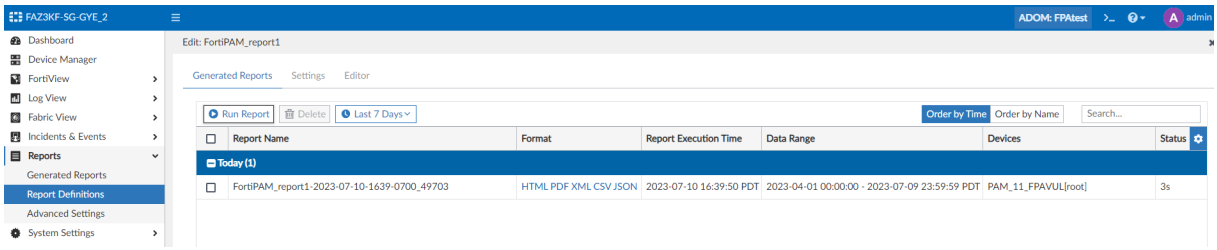
The FortiPAM device is now authorized in *Device Manager*.



3. To view logs from the FortiPAM device, go to *Log View* > *FortiPAM*.



You can create a FortiPAM report in FortiAnalyzer.

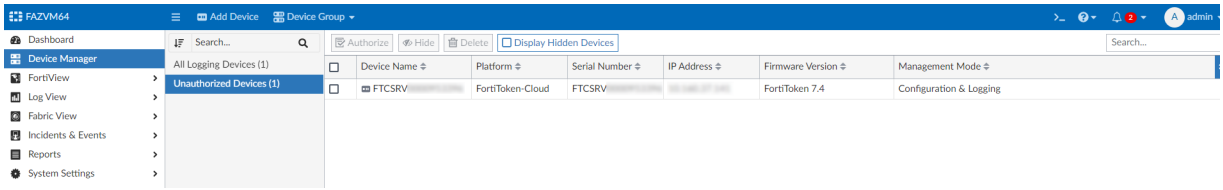


Logging support for FortiToken Cloud - 7.4.1

FortiAnalyzer can now receive, store, and display logs from authorized FortiToken Cloud devices in *Log View*.

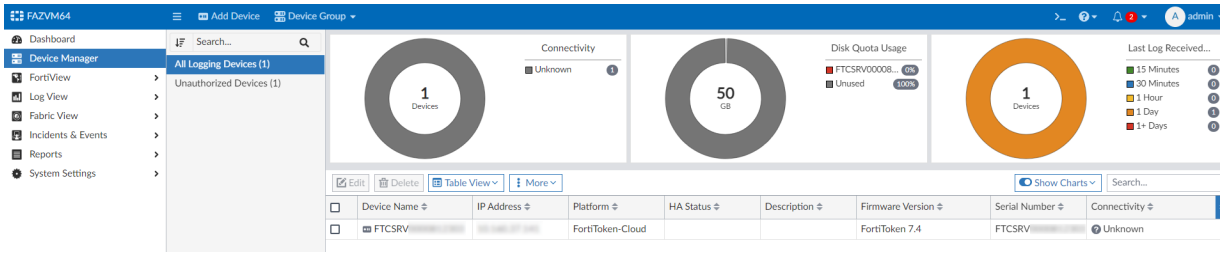
To configure FortiToken Cloud logging on FortiAnalyzer:

1. Configure the FortiToken Cloud device to send logs to FortiAnalyzer.
2. In the FortiAnalyzer GUI, go to *Device Manager* in the root ADOM.
   The FortiToken Cloud displays in the *Unauthorized Devices* list.

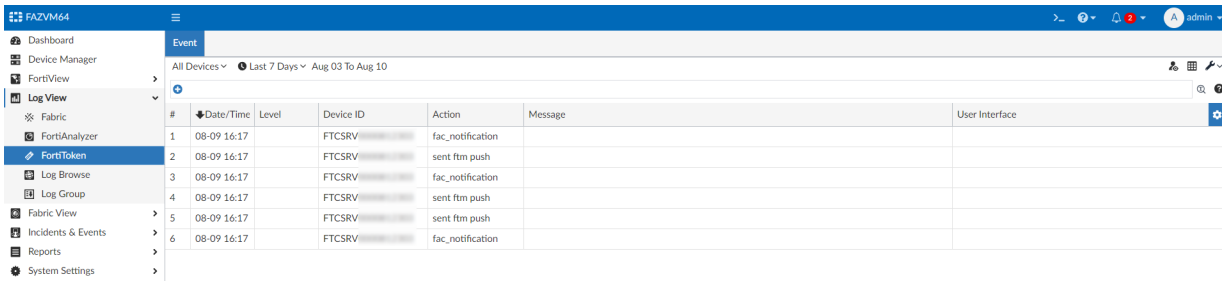


3. Select the FortiToken Cloud device and click *Authorize*.

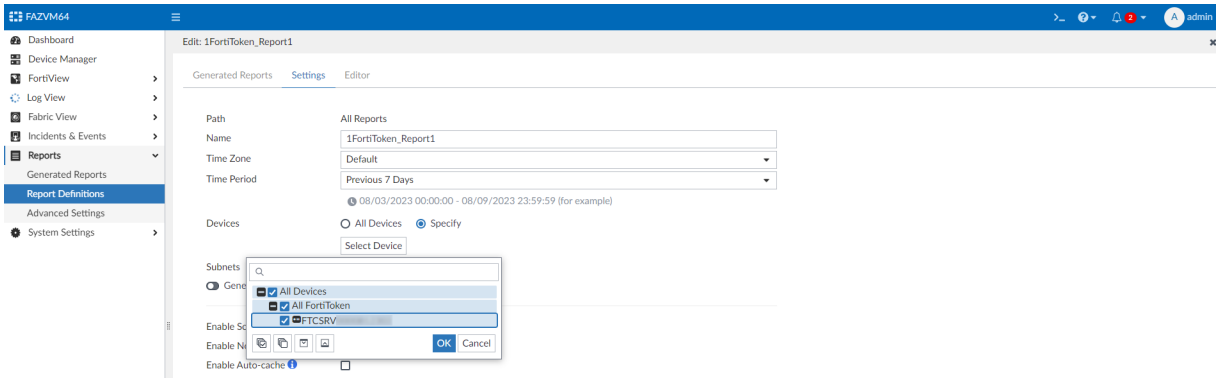
The FortiToken Cloud device now displays in *All Logging Devices* list.



The FortiToken Cloud logs display in *Log View* > *FortiToken*.



The FortiToken Cloud device can now be used in *Reports*.



Log Forwarding

This section lists the new features added to FortiAnalyzer for log forwarding:

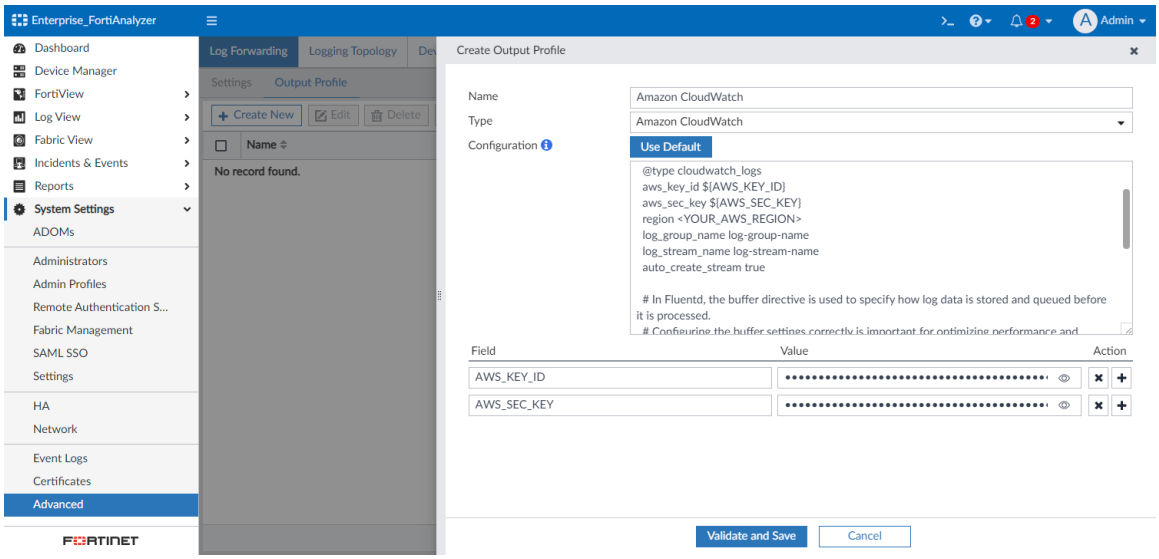
- Fluentd support for public cloud integration on page 30

Fluentd support for public cloud integration

You can create output profiles to configure log forwarding to public cloud services.

To create an output profile for log forwarding:

1. Go to *System Settings* > *Advanced* > *Log Forwarding* > *Output Profile*.
2. Click *Create New*.
   The *Create Output Profile* pane displays.



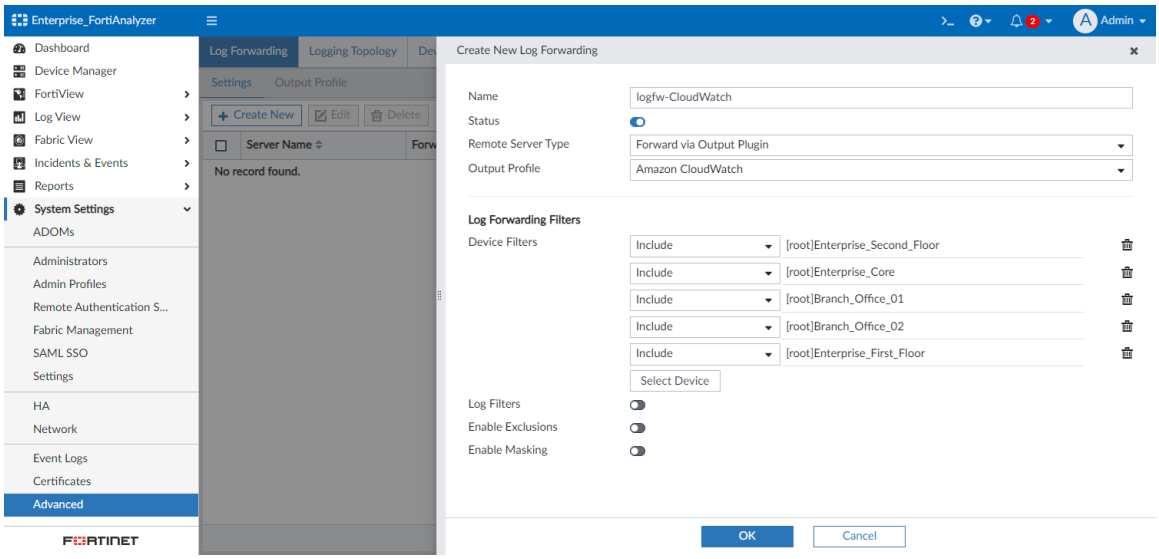
3. Configure the following options:

Name	Enter a name for the output profile.
Type	Select the public cloud service for the output profile.
Configuration	Click *Use Default* to use the default Fluentd configuration for the selected public cloud service. Alternatively, copy and paste the Fluentd configuration into this field for the selected public cloud service.
Field	Fields will automatically be added into the configuration if a keyword matches the placeholder in the configuration to provide encryption for you to hide the credentials. For example, a password placeholder in the configuration would be "`${password}`". In the field, you can define *Field*: `password`, *Value*: `actual_password`.

4. Click *Validate and Save*.

To configure log forwarding to the output profile:

1. Go to *System Settings* > *Advanced Log Forwarding* > *Settings*.
2. Click *Create New*.
   The *Create New Log Forwarding* pane displays.



3. Configure the following options:

Name	Enter a name for the remote server.
Status	Enable log forwarding.
Remote Server Type	Select *Forward via Output Plugin*.
Output Profile	Select the output profile.
Log Forwarding Filters	
Device Filters	Click *Select Device*, then select the devices whose logs will be forwarded.
Log Filters	Enable to configure filters for the logs that are forwarded.
Enable Exclusions	Enable to configure filter on the logs that are forwarded.
Enable Masking	Enable log field masking, if needed.

4. Click *OK*.

To troubleshoot the Fluentd connection with the FortiAnalyzer CLI:

1. In the FortiAnalyzer CLI, enter the following command to check the Fluentd write status:

```
FAZVM64 # diagnose test application fwdplugind 4
   Stats for plugin:
   lfw_name: logfw-CloudWatch
   plugin_name: Amazon CloudWatch
   type: AMAZON_CLOUDWATCH
   fd-plug-id: tcp_1_3da_6af_922_1c3
   fluentd emit stats(emit_calls|emit_rec_calls|emit_size): 3685, 88677, 0
   fluentd write stats(write|retry|rollback): 3, 0, 0
   fluentd buffer queue(byte_size|total_queue_size|queue_len|ratio): 49842536,
        52433884, 2, 0
   fluentd buffer stage(byte_size|stage_length): 4325288, 1
   fluentd flush stats(flush_time|slow_flush_count): 0, 0
```

2. In the FortiAnalyzer CLI, enter the following command to determine if the Fluentd log files are present:

```
FAZVM64 # diagnose sql fluentd log-tail
   Fluentd log files are not present. Please turn on Fluentd log first if you need to
        test it.
```

3. In the FortiAnalyzer CLI, enter the following command to enable Fluentd logging:

```
FAZVM64 # diagnose test application fwdplugind 201 log enable
   Warning: This will enable Fluentd logging.
   Fluentd requires a restart for changes to take effect. The restart will disrupt
        Fluentd's current log handling.
   Execute the command again in one minute for the changes to take effect.
FAZVM64 # diagnose test application fwdplugind 201 log enable
   Fluentd logging is enabled, Fluentd will be restarted.
```

4. In the FortiAnalyzer CLI, enter the following command again to show the processed events:

```
FAZVM64 # diagnose sql fluentd log-tail
   File /drive0/private/fwdplugind/fluentd/logs/faz-td-agent.log, is present, will
        open it.
   Please press Control+C to exit.
   ====================================
   aws_sec_key xxxxxx
   region "us-west-2"
   log_group_name "Log-Group-Test"
   log_stream_name "Log-Stream-test"
   auto_create_stream true
   @id tcp_1_3da_6af_922_1c3
   <buffer tag,time>
   @type "memory"
   chunk_limit_size 10M
   total_limit_size 50M
   timekey 5m
   timekey_wait 30s
   timekey_use_utc true
   flush_thread_count 3
   flush_at_shutdown true
   overflow_action block
   retry_forever true
   disable_chunk_backup true
   </buffer>
   </match>
   </worker>
   </ROOT>
   2023-04-24 16:05:20 -0700 [info]: starting fluentd-1.15.2 pid=12376 ruby="2.7.6"
   2023-04-24 16:05:20 -0700 [info]: spawn command to main: cmdline=
        ["/usr/local/fluentd/td-agent/bin/ruby", "-Eascii-8bit:ascii-8bit",
        "/usr/sbin/td-agent", "-d", "/drive0/private/fwdplugind/fluentd/faz-td-
        agent.pid", "-c", "/drive0/private/fwdplugind/fluentd/faz-td-agent.conf", "-
        o", "/drive0/private/fwdplugind/fluentd/logs/faz-td-agent.log", "--log-rotate-
        size", "5120000", "--under-supervisor"]
   2023-04-24 16:05:20 -0700 [info]: #0 adding match pattern="tcp_1" type="cloudwatch_
        logs"
   2023-04-24 16:05:21 -0700 [info]: adding source type="monitor_agent"
   2023-04-24 16:05:21 -0700 [info]: #0 adding source type="tcp"
   2023-04-24 16:05:21 -0700 [info]: #0 starting fluentd worker pid=12390 ppid=12387
        worker=0
   2023-04-24 16:05:21 -0700 [info]: #0 listening tcp socket bind="127.0.0.1"
        port=10000
   2023-04-24 16:05:21 -0700 [info]: #0 fluentd worker is now running worker=0
```

Reports

This section lists the new features added to FortiAnalyzer for reports:

- Report guidance on page 34
- PCI Security Rating Report on page 36
- Cyber Threats Assessment Report update on page 37
- Threat Report update on page 38
- FSBP Security Rating Report on page 40
- CIS Controls Security Rating report on page 41
- Shadow IT Report on page 42
- FortiADC Report 7.4.1 on page 43
- Default ZTNA Report 7.4.1 on page 45

Report guidance

This information is also available in the FortiAnalyzer 7.4 Administration Guide:
- Report guidance

FortiAnalyzer provides many factory default reports that use charts relying on specific log types and log fields to provide valuable output. When running a full report, you may see "`No Data`" returned in sections if:

- logging was not enabled correctly
- the report element is for a different Device/Log Type
- there are no matching logs

Debugging such scenarios can be time consuming because it requires navigating through charts, macros, and datasets.

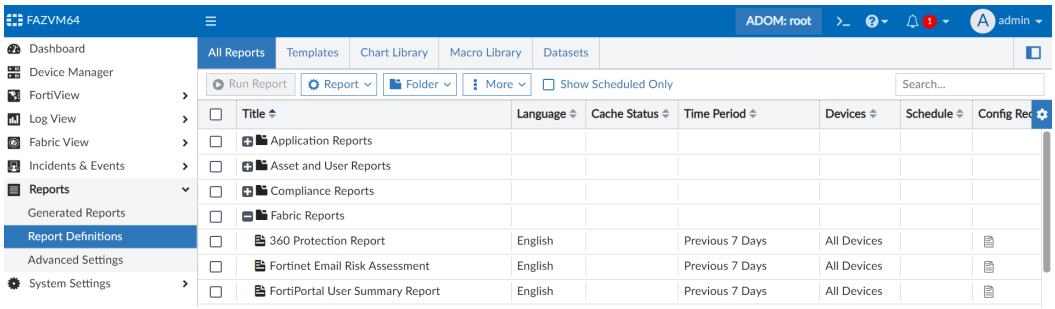
To improve the overall reporting experience, a new *Report Guidance* feature has been implemented to provide full visibility for each report element in terms of:

- Device Type (e.g. Fortigate)
- Log Type (e.g. traffic)
- Log Fields (e.g. action, itime)

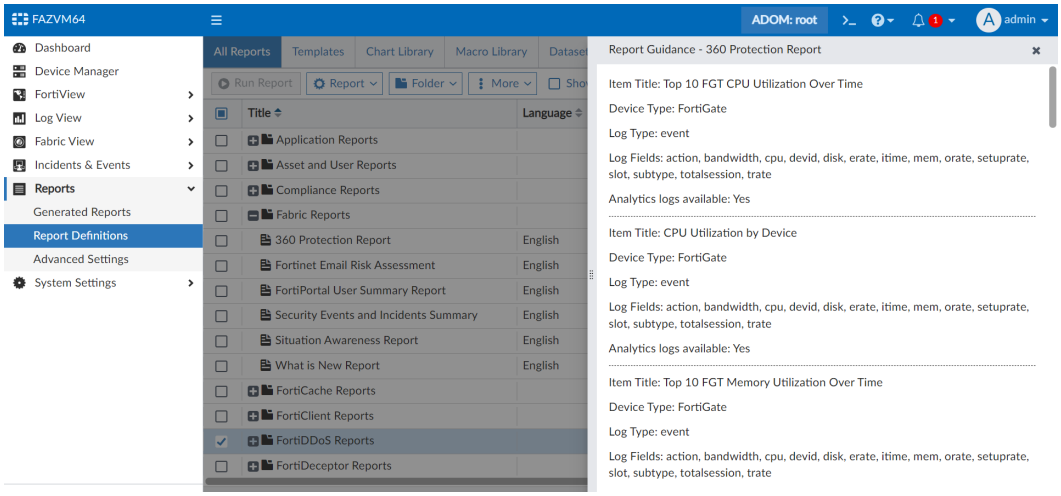
In short, you can use the *Report Guidance* feature to troubleshoot and determine if FortiAnalyzer has the appropriate Analytics logs available for a report.

To use the Report Guidance feature:

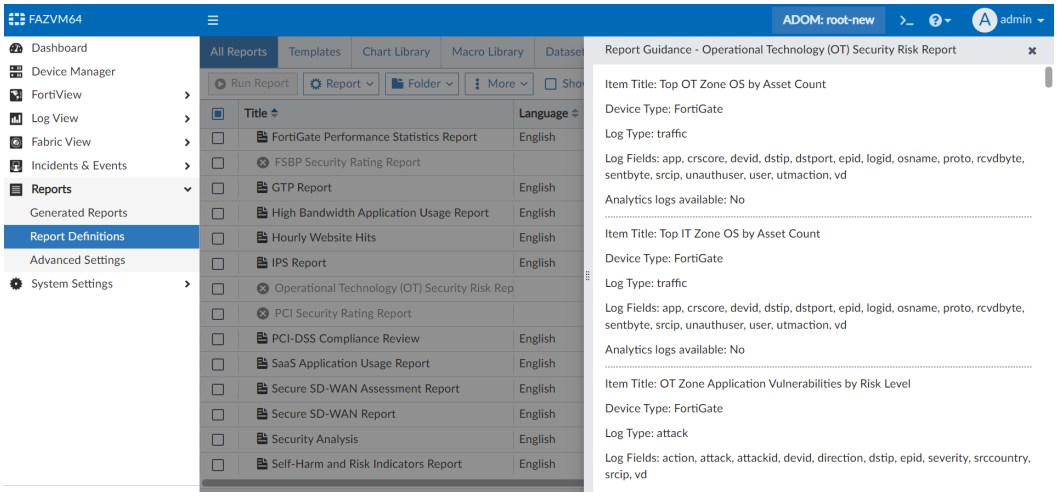
1. Go to *Reports* > *Report Definitions* > *All Reports*.
   There is a new *Config Recommendation* column.



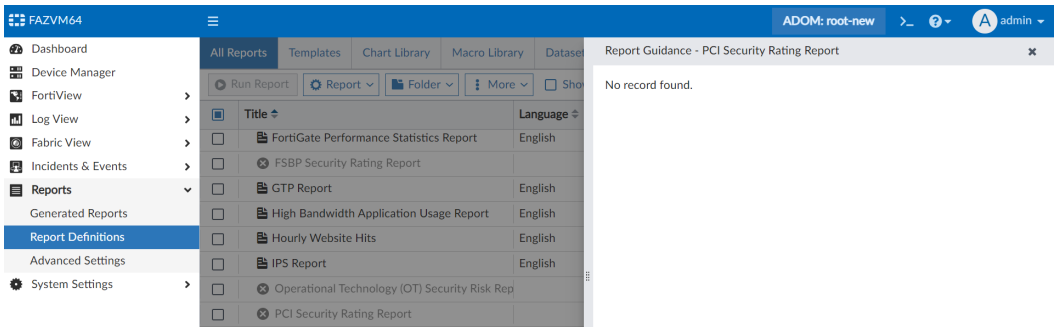
2. Click the icon in the *Config Recommendation* column.
   The *Report Guidance* pane opens for that report. This pane provides the `Item Title` (chart or macro name), `Device Type`, `Log Type`, and the relevant `Log Fields` and Analytics log availability.



The *Report Guidance* pane is available for license-controlled reports, but the report cannot be generated without a valid license.



For reports that are not generated with log tables, such as the FSBP/PCI or CIS Security Rating Reports, the *Report Guidance* pane will indicate `No record found`.

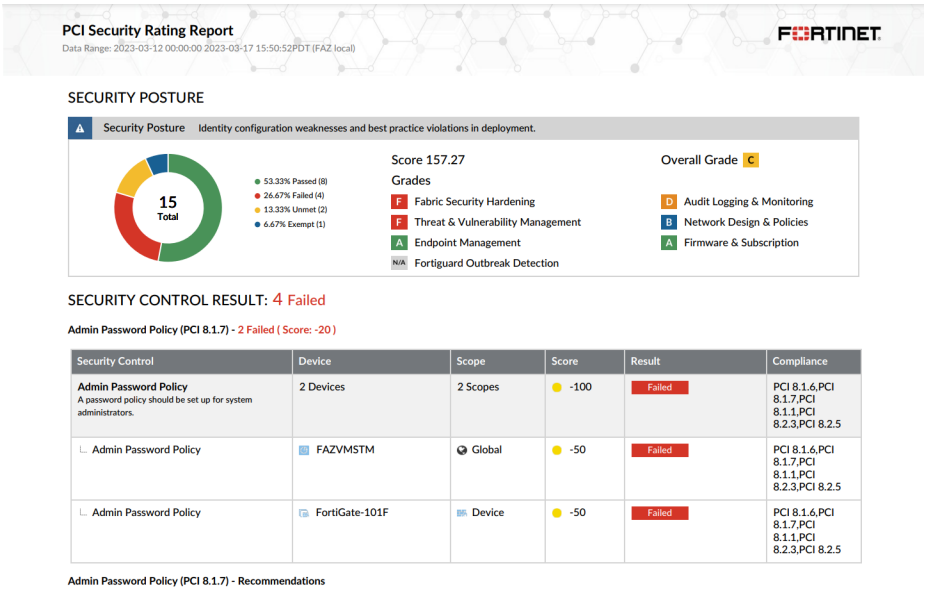


PCI Security Rating Report

A *PCI Security Rating Report* is now available on FortiAnalyzer to optimize the deployed FortiGates in terms of *Security Posture*, *Fabric Coverage*, and *Optimization* based on PCI DSS 3.2 standards. This report consolidates security ratings performed on fabric deployments.

Each category includes the *Failed*, *Unmet*, *Passed*, and *Exempt* security control results. Recommendations are provided as well.

For example, see a sample of page 1 from the report in PDF format below.


PCI Security Rating Report

Data Range: 2023-03-12 00:00:00 2023-03-17 15:50:52PDT (FAZ local)

FORTINET

SECURITY POSTURE

Security Posture Identity configuration weaknesses and best practice violations in deployment.

15 Total

53.33% Passed (8)
26.67% Failed (4)
13.33% Unmet (2)
6.67% Exempt (1)

Score 157.27

Grades

F Fabric Security Hardening
F Threat & Vulnerability Management
A Endpoint Management
N/A Fortiguard Outbreak Detection

Overall Grade C

D Audit Logging & Monitoring
B Network Design & Policies
A Firmware & Subscription

SECURITY CONTROL RESULT: 4 Failed

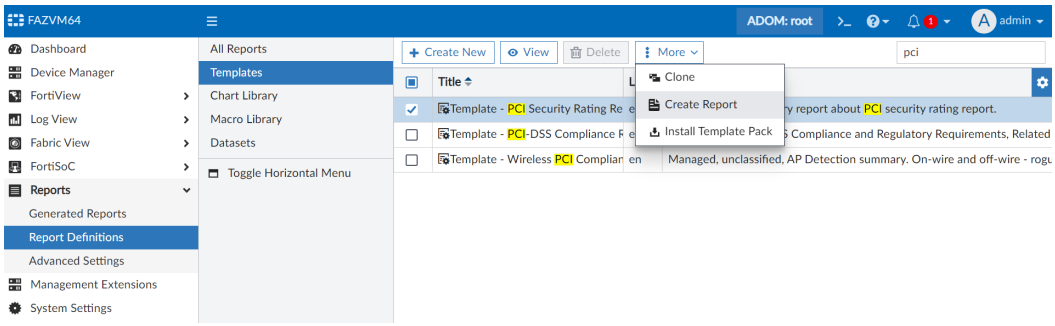
Admin Password Policy (PCI 8.1.7) - 2 Failed (Score: -20)

Security Control	Device	Scope	Score	Result	Compliance
Admin Password Policy A password policy should be set up for system administrators.	2 Devices	2 Scopes	-100	Failed	PCI 8.1.6,PCI 8.1.7,PCI 8.1.1,PCI 8.2.3,PCI 8.2.5
Admin Password Policy	FAZVMSTM	Global	-50	Failed	PCI 8.1.6,PCI 8.1.7,PCI 8.1.1,PCI 8.2.3,PCI 8.2.5
Admin Password Policy	FortiGate-101F	Device	-50	Failed	PCI 8.1.6,PCI 8.1.7,PCI 8.1.1,PCI 8.2.3,PCI 8.2.5

Admin Password Policy (PCI 8.1.7) - Recommendations

To create the report from the template:

1. Go to *Reports* > *Report Definitions* > *Templates*.
   From the *Preview* column, you can click *PDF* or *HTML* to preview the report in that format.
2. Select the checkbox for *Template - PCI Security Rating Report*.
3. From the *More* dropdown, click *Create Report* to create a report using the template.
   You can also click *Clone* to clone the template and make adjustments.



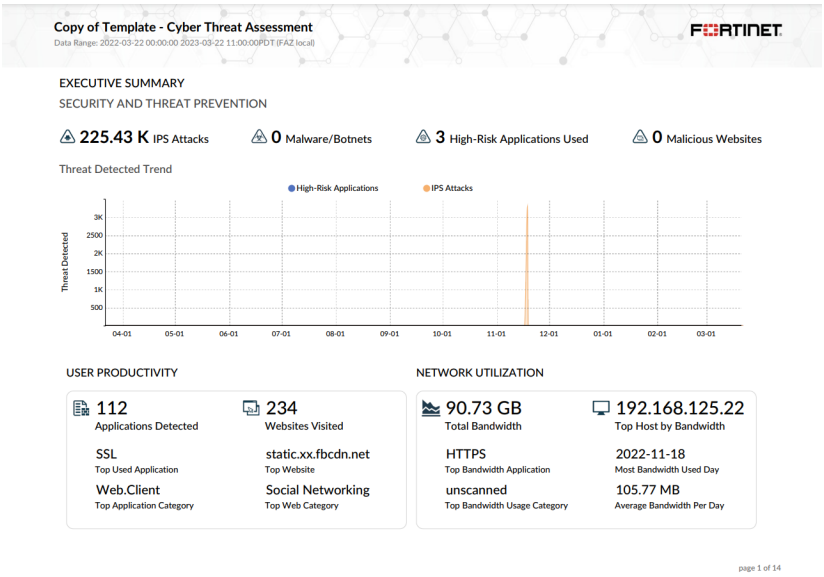
To run the PCI Security Rating Report:

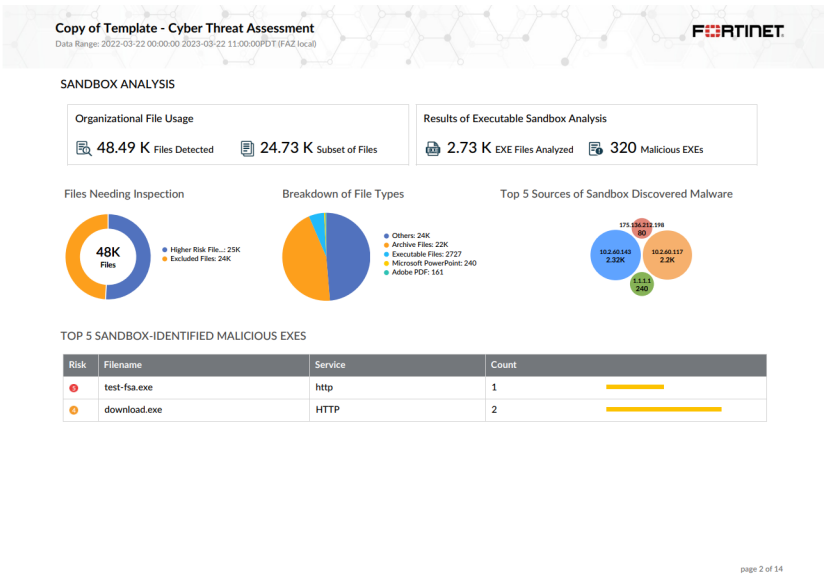
1. Go to *Reports* > *Report Definitions* > *All Reports*, and double-click the row for the *PCI Security Rating Report*.
   The *Edit: PCI Security Rating Report* pane opens.
2. Click *Run Report*.
   Once the report is available, click the format to view the report in.

Cyber Threats Assessment Report update

The existing *Cyber Threats Assessment Report* has been updated with new style and content to enhance the visibility of the provided data.

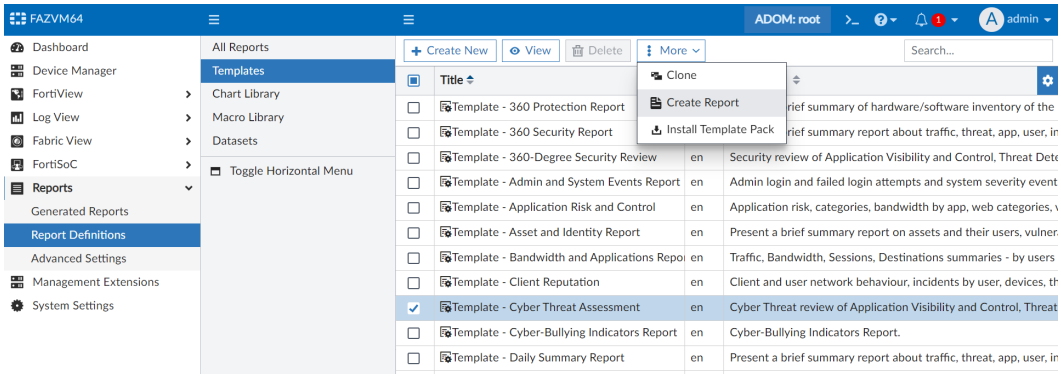
For example, see a sample of the report in PDF format below:





To create the report from the template:

1. Go to *Reports* > *Report Definitions* > *Templates*.
   From the *Preview* column, you can click *PDF* or *HTML* to preview the report in that format.
2. Select the checkbox for *Template - Cyber Threats Assessment Report*.
3. From the *More* dropdown, click *Create Report* to create a report using the template.
   You can also click *Clone* to clone the template and make adjustments.



To run the Cyber Threats Assessment Report:

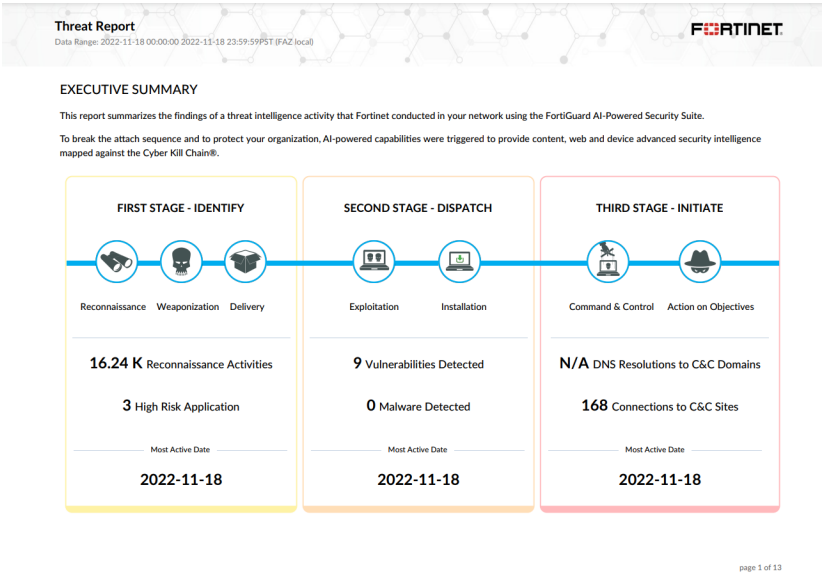
1. Go to *Reports* > *Report Definitions* > *All Reports*, and double-click the row for the *Cyber Threats Assessment Report*.
   The *Edit: Cyber Threats Assessment Report* pane opens.
2. Click *Run Report*.
   Once the report is available, click the format to view the report in.

Threat Report update

The *Threat Report* has been updated to provide the following:

- New style and content to better present threat data
- Threats are mapped to the Cyber Kill Chain stages for correlation and pattern identification

For example, see a sample of the report in PDF format below:



Threat Report
Data Range: 2022-11-18 00:00:00 2022-11-18 23:59:59PST (FAZ local)

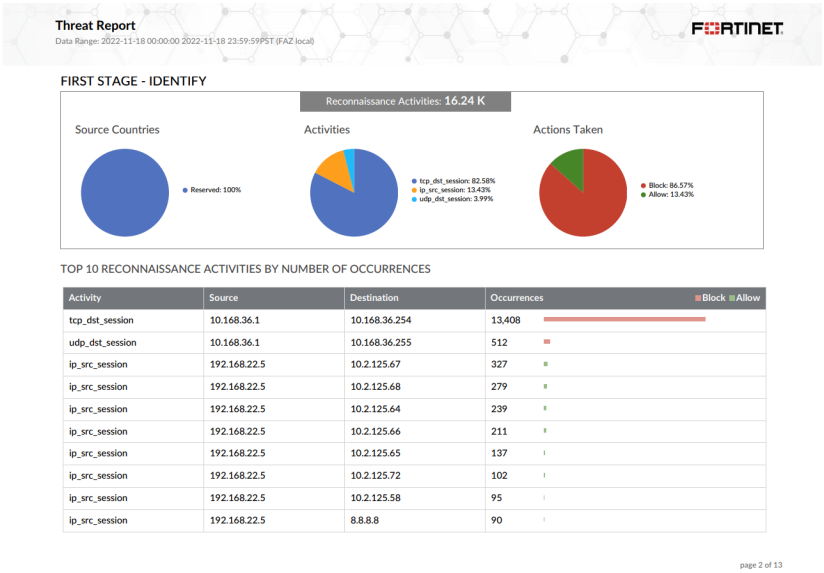
EXECUTIVE SUMMARY

This report summarizes the findings of a threat intelligence activity that Fortinet conducted in your network using the FortiGuard AI-Powered Security Suite.

To break the attach sequence and to protect your organization, AI-powered capabilities were triggered to provide content, web and device advanced security intelligence mapped against the Cyber Kill Chain®.

FIRST STAGE - IDENTIFY	SECOND STAGE - DISPATCH	THIRD STAGE - INITIATE
Reconnaissance Weaponization Delivery	Exploitation Installation	Command & Control Action on Objectives
16.24 K Reconnaissance Activities	**9** Vulnerabilities Detected	**N/A** DNS Resolutions to C&C Domains
3 High Risk Application	**0** Malware Detected	**168** Connections to C&C Sites
Most Active Date	Most Active Date	Most Active Date
2022-11-18	**2022-11-18**	**2022-11-18**

page 1 of 13



Threat Report
Data Range: 2022-11-18 00:00:00 2022-11-18 23:59:59PST (FAZ local)

FIRST STAGE - IDENTIFY

Reconnaissance Activities: **16.24 K**

Source Countries — Reserved: 100%

Activities — tcp_dst_session: 82.58%; ip_src_session: 13.43%; udp_dst_session: 3.99%

Actions Taken — Block: 86.57%; Allow: 13.43%

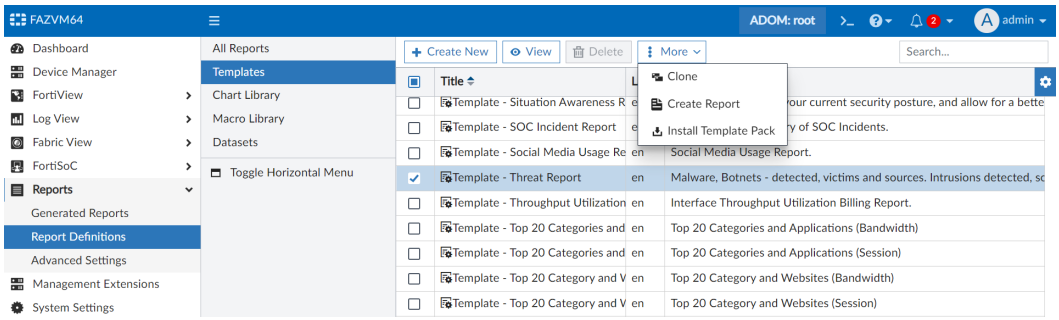
TOP 10 RECONNAISSANCE ACTIVITIES BY NUMBER OF OCCURRENCES

Activity	Source	Destination	Occurrences (Block / Allow)
tcp_dst_session	10.168.36.1	10.168.36.254	13,408
udp_dst_session	10.168.36.1	10.168.36.255	512
ip_src_session	192.168.22.5	10.2.125.67	327
ip_src_session	192.168.22.5	10.2.125.68	279
ip_src_session	192.168.22.5	10.2.125.64	239
ip_src_session	192.168.22.5	10.2.125.66	211
ip_src_session	192.168.22.5	10.2.125.65	137
ip_src_session	192.168.22.5	10.2.125.72	102
ip_src_session	192.168.22.5	10.2.125.58	95
ip_src_session	192.168.22.5	8.8.8.8	90

page 2 of 13

To create the report from the template:

1. Go to *Reports* > *Report Definitions* > *Templates*.
   From the *Preview* column, you can click *PDF* or *HTML* to preview the report in that format.
2. Select the checkbox for *Template - Threat Report*.
3. From the *More* dropdown, click *Create Report* to create a report using the template.
   You can also click *Clone* to clone the template and make adjustments.



To run the Threat Report:

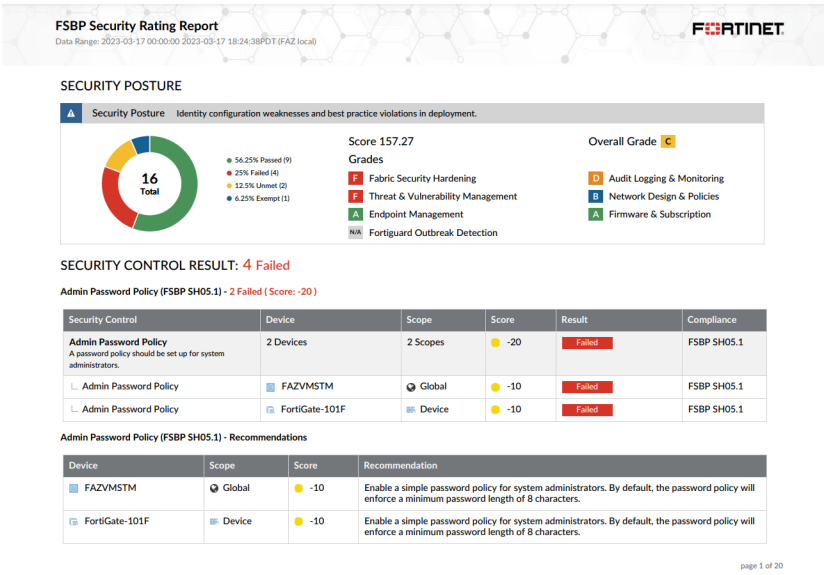
1. Go to *Reports* > *Report Definitions* > *All Reports*, and double-click the row for the *Threat Report*.
   The *Edit: Threat Report* pane opens.
2. Click *Run Report*.
   Once the report is available, click the format to view the report in.

FSBP Security Rating Report

A FSBP (Fortinet Security Best Practices) Security Rating Report is available on FortiAnalyzer to optimize the deployed FortiGates in terms of *Security Posture*, *Fabric Coverage*, and *Optimization*. This report consolidates security ratings performed on fabric deployments.

Each category includes the *Failed*, *Unmet*, *Passed*, and *Exempt* security control results. Recommendations are provided as well.

For example, see a sample of page 1 from the report in PDF format below.


FSBP Security Rating Report

Data Range: 2023-03-17 00:00:00 2023-03-17 18:24:38PDT (FAZ local)

FORTINET

SECURITY POSTURE

Security Posture Identity configuration weaknesses and best practice violations in deployment.

16 Total

56.25% Passed (9)
25% Failed (4)
12.5% Unmet (2)
6.25% Exempt (1)

Score 157.27

Overall Grade C

Grades

F Fabric Security Hardening
F Threat & Vulnerability Management
A Endpoint Management
N/A Fortiguard Outbreak Detection
D Audit Logging & Monitoring
B Network Design & Policies
A Firmware & Subscription

SECURITY CONTROL RESULT: 4 Failed

Admin Password Policy (FSBP SH05.1) - 2 Failed (Score: -20)

Security Control	Device	Scope	Score	Result	Compliance
Admin Password Policy A password policy should be set up for system administrators.	2 Devices	2 Scopes	-20	Failed	FSBP SH05.1
Admin Password Policy	FAZVMSTM	Global	-10	Failed	FSBP SH05.1
Admin Password Policy	FortiGate-101F	Device	-10	Failed	FSBP SH05.1

Admin Password Policy (FSBP SH05.1) - Recommendations

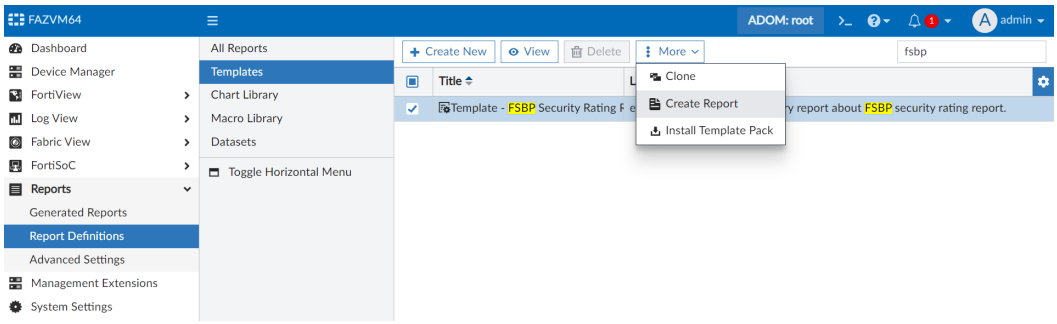
Device	Scope	Score	Recommendation
FAZVMSTM	Global	-10	Enable a simple password policy for system administrators. By default, the password policy will enforce a minimum password length of 8 characters.
FortiGate-101F	Device	-10	Enable a simple password policy for system administrators. By default, the password policy will enforce a minimum password length of 8 characters.

page 1 of 20

To create the report from the template:

1. Go to *Reports* > *Report Definitions* > *Templates*.
   From the *Preview* column, you can click *PDF* or *HTML* to preview the report in that format.

2. Select the checkbox for *Template - FSBP Security Rating Report*.
3. From the *More* dropdown, click *Create Report* to create a report using the template.
   You can also click *Clone* to clone the template and make adjustments.



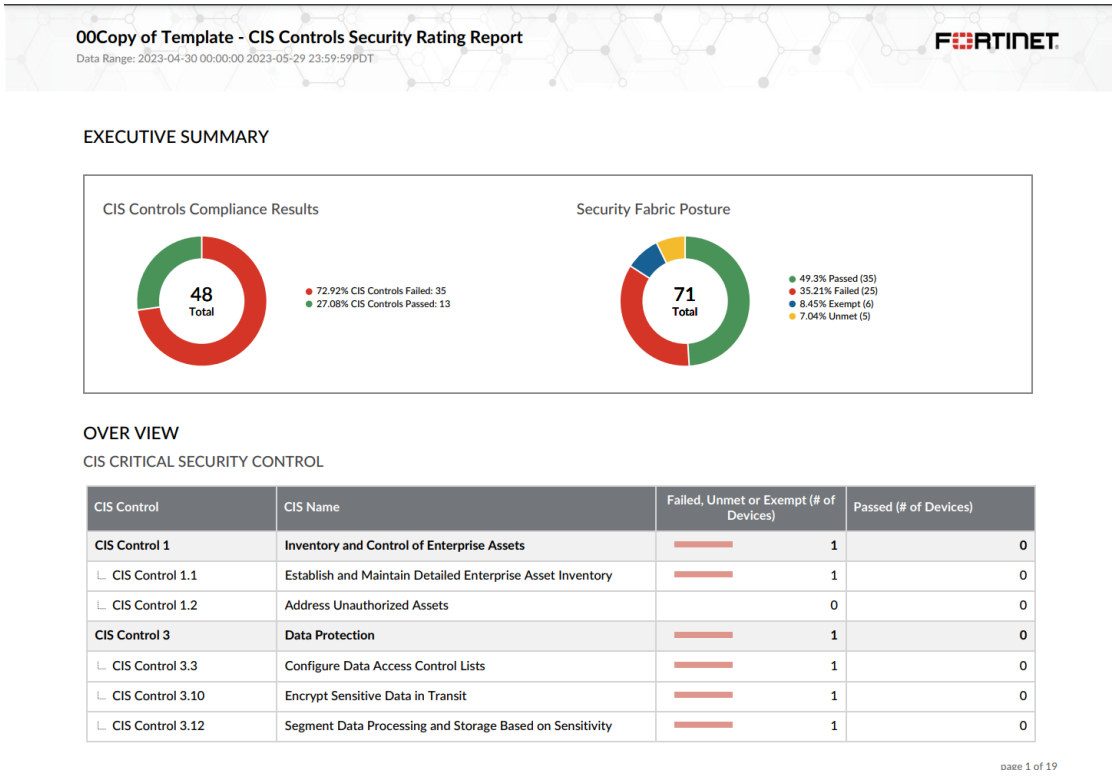
To run the FSBP Security Rating Report:

1. Go to *Reports* > *Report Definitions* > *All Reports*, and double-click the row for the *FSBP Security Rating Report*.
   The *Edit: FSBP Security Rating Report* pane opens.
2. Click *Run Report*.
   Once the report is available, click the format to view the report in.

CIS Controls Security Rating report

A *CIS Controls Security Rating Report* is now available on FortiAnalyzer. This report includes CIS mapping information.

For example, see a sample of the report in PDF format below.



00Copy of Template - CIS Controls Security Rating Report

Data Range: 2023-04-30 00:00:00 2023-05-29 23:59:59PDT

FORTINET

EXECUTIVE SUMMARY

CIS Controls Compliance Results

Security Fabric Posture

OVER VIEW

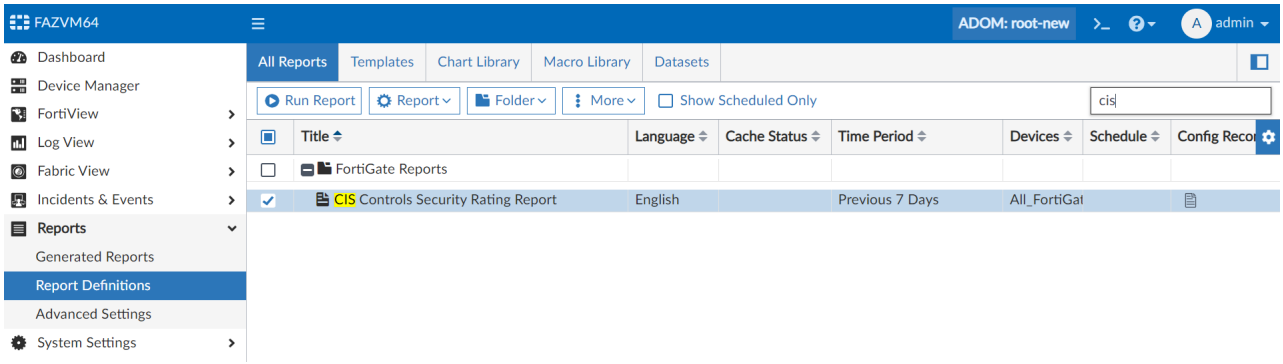
CIS CRITICAL SECURITY CONTROL

CIS Control	CIS Name	Failed, Unmet or Exempt (# of Devices)	Passed (# of Devices)
CIS Control 1	**Inventory and Control of Enterprise Assets**	1	0
CIS Control 1.1	Establish and Maintain Detailed Enterprise Asset Inventory	1	0
CIS Control 1.2	Address Unauthorized Assets	0	0
CIS Control 3	**Data Protection**	1	0
CIS Control 3.3	Configure Data Access Control Lists	1	0
CIS Control 3.10	Encrypt Sensitive Data in Transit	1	0
CIS Control 3.12	Segment Data Processing and Storage Based on Sensitivity	1	0

page 1 of 19

To create the report from the template:

1. Go to *Reports* > *Report Definitions* > *Templates*.
   From the *Preview* column, you can click *PDF* or *HTML* to preview the report in that format.
2. Select the checkbox for *Template - CIS Controls Security Rating Report*.
3. From the *More* dropdown, click *Create Report* to create a report using the template.
   You can also click *Clone* to clone the template and make adjustments.



To run the CIS Controls Security Rating Report:

1. Go to *Reports* > *Report Definitions* > *All Reports*, and double-click the row for the *CIS Controls Security Rating Report*.
   The *Edit: CIS Controls Security Rating Report* pane opens.
2. Click *Run Report*.
   Once the report is available, click the format to view the report in.

Shadow IT Report

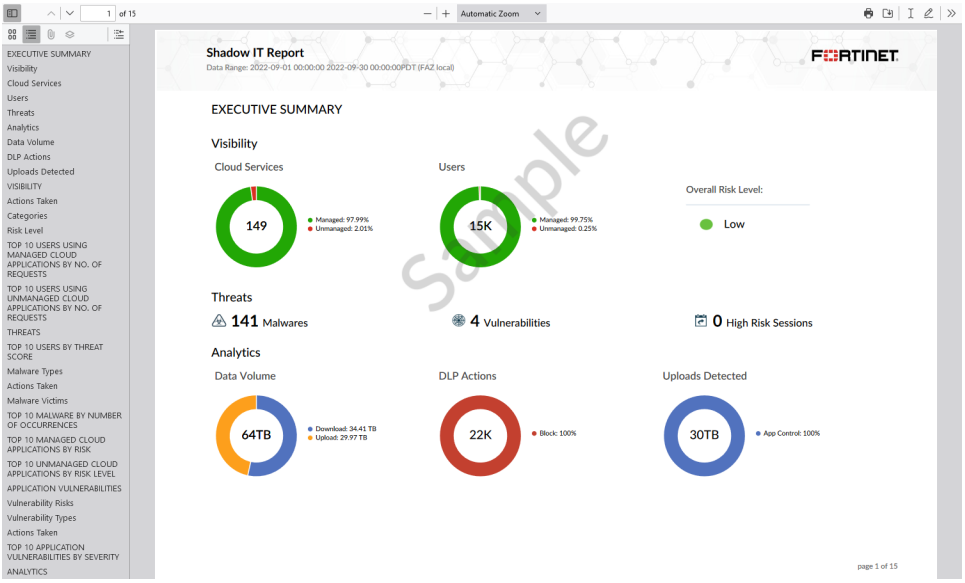
The *Shadow IT Report* is now available on FortiAnalyzer.

This report provides enhanced visibility and control for cloud based applications.

Detected applications are classified as:

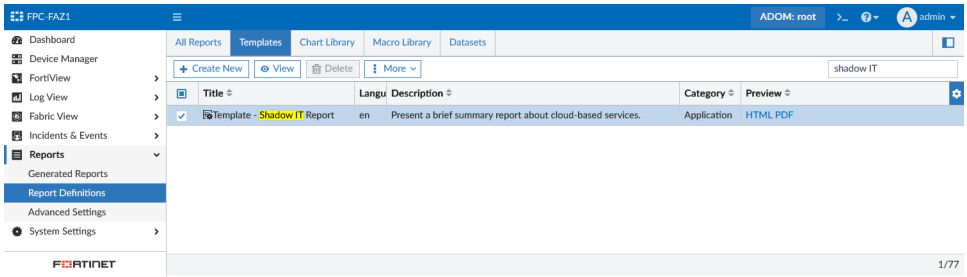
- Managed > Allowed
- Unmanaged > Blocked/Quarantined/Reset

For example, see a sample of page 1 from the report in PDF format below.



To create the report from the template:

1. Go to *Reports* > *Report Definitions* > *Templates*.
   From the *Preview* column, you can click *PDF* or *HTML* to preview the report in that format.
2. Select the checkbox for *Template - Shadow IT Report*.
3. From the *More* dropdown, click *Create Report* to create a report using the template.
   You can also click *Clone* to clone the template and make adjustments.



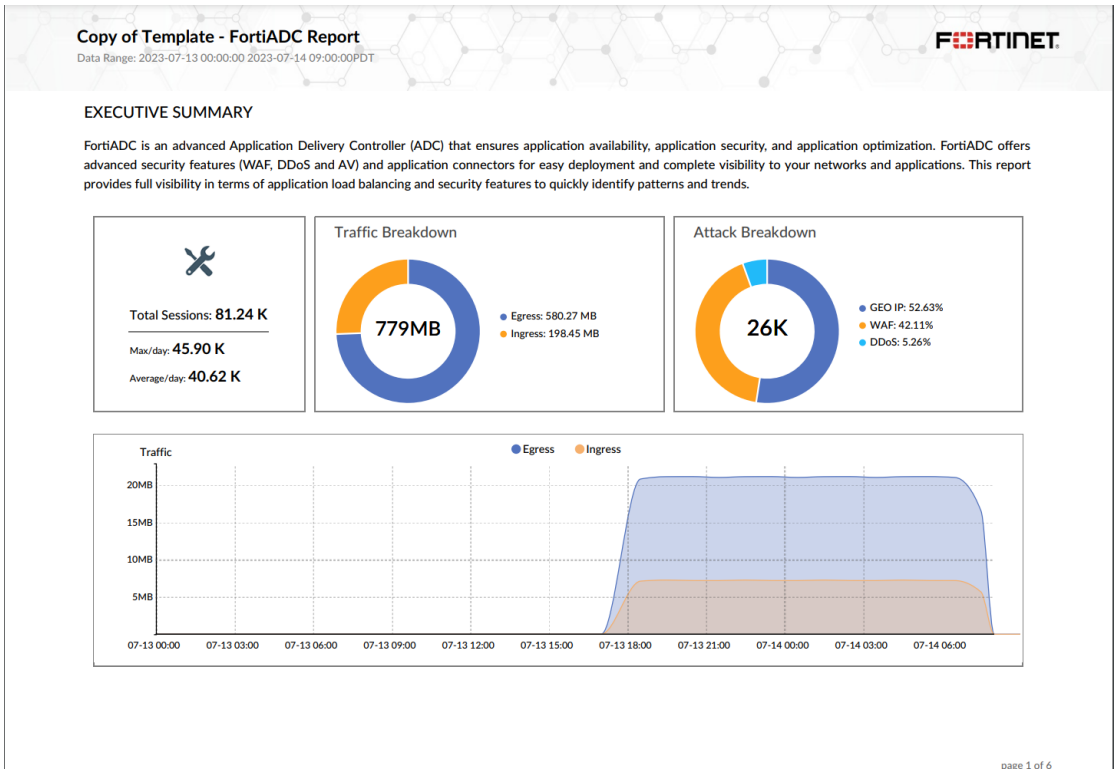
To run the Shadow IT Report:

1. Go to *Reports* > *Report Definitions* > *All Reports*, and double-click the row for the *Shadow IT Report*.
   The *Edit: Shadow IT Report* pane opens.
2. Click *Run Report*.
   Once the report is available, click the format to view the report in.

FortiADC Report - 7.4.1

The *FortiADC Report* is available on FortiAnalyzer to offer comprehensive visibility into application load balancing and security features, enabling rapid identification of security patterns and trends associated with the use of the product.

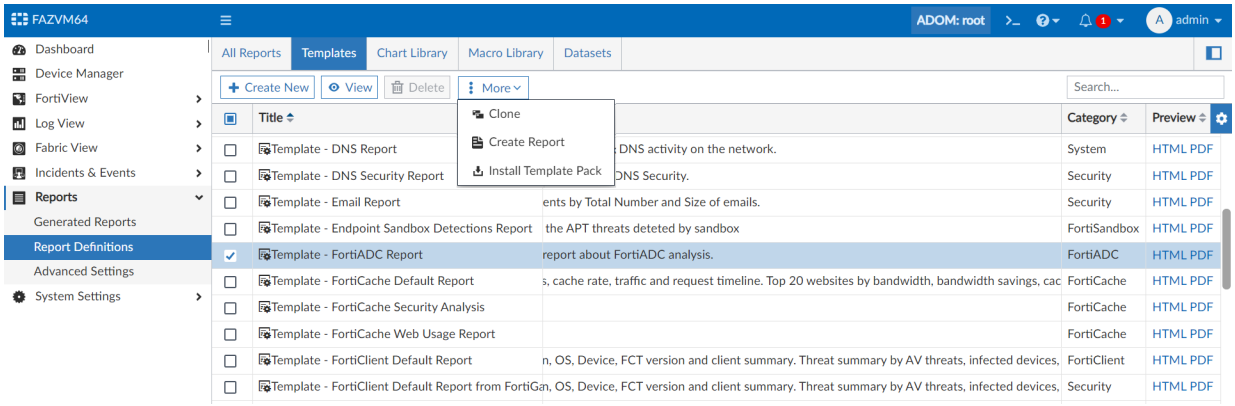
For example, see a sample of page 1 from the report in PDF format below.



This report requires that a FortiADC device has been added and authorized to the FortiAnalyzer.

To create the report from the template:

1. Go to *Reports* > *Report Definitions* > *Templates*.
   From the *Preview* column, you can click *PDF* or *HTML* to preview the report in that format.
2. Select the checkbox for *Template - FortiADC Report*.
3. From the *More* dropdown, click *Create Report* to create a report using the template.
   You can also click *Clone* to clone the template and make adjustments.



To run the FortiADC Report:

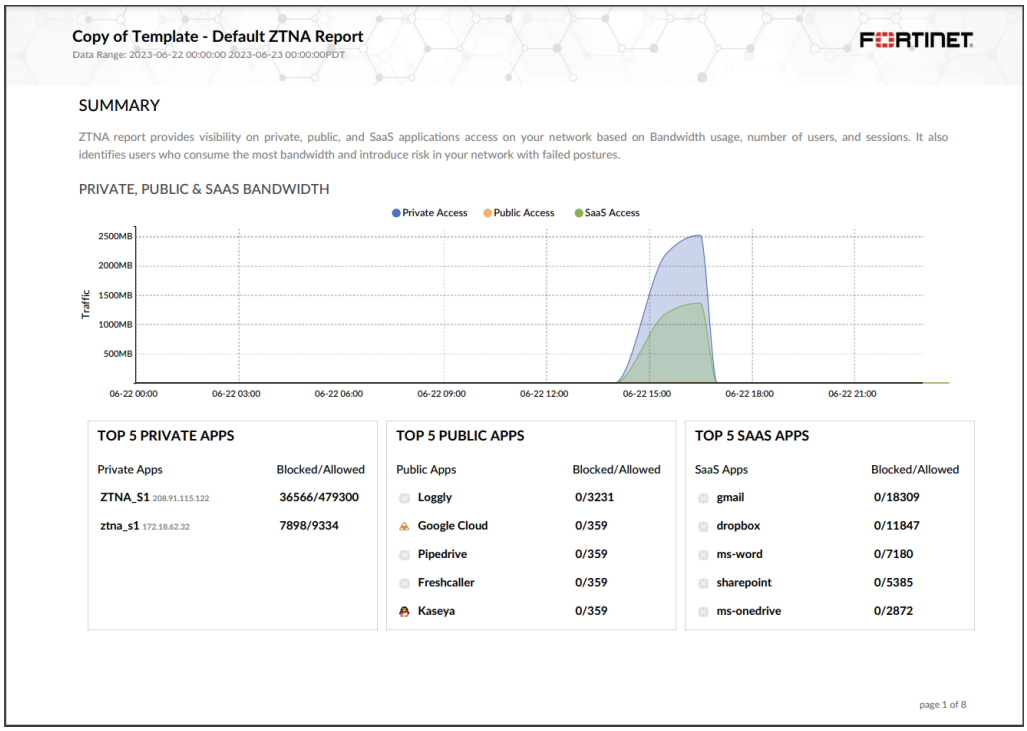
1. Go to *Reports* > *Report Definitions* > *All Reports*, and double-click the row for the *FortiADC Report*.
   The *Edit: FortiADC Report* pane opens.

2. Click *Run Report*.
   Once the report is available, click the format to view the report in.

Default ZTNA Report - 7.4.1

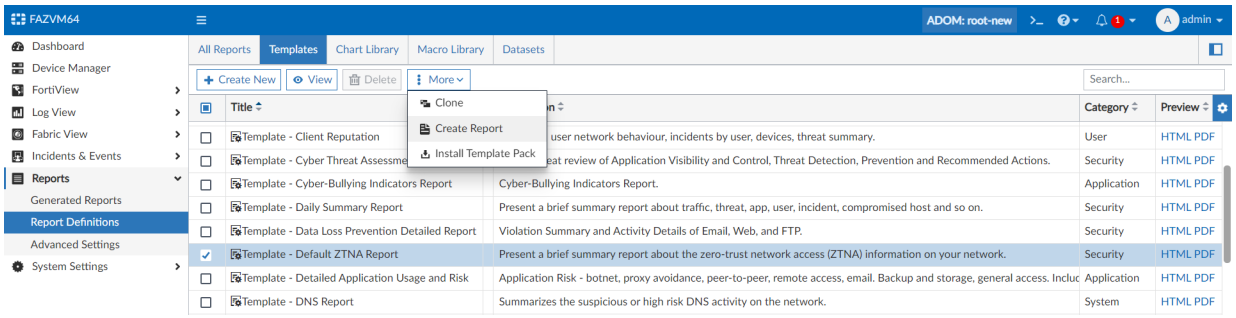
The *Default ZTNA Report* is now available on FortiAnalyzer to enhance visibility in terms of applications being used with the corresponding bandwidth used and sessions. To better differentiate accessibility and deployments, applications are grouped as private, public, and SaaS. Users that present security risks due to failing security postures can be quickly identified.

For example, see a sample of page 1 from the report in PDF format below.



To create the report from the template:

1. Go to *Reports* > *Report Definitions* > *Templates*.
   From the *Preview* column, you can click *PDF* or *HTML* to preview the report in that format.
2. Select the checkbox for *Template - Default ZTNA Report*.
3. From the *More* dropdown, click *Create Report* to create a report using the template.
   You can also click *Clone* to clone the template and make adjustments.



To run the Default ZTNA Report:

1. Go to *Reports* > *Report Definitions* > *All Reports*, and double-click the row for the *Default ZTNA Report*.
   The *Edit: Default ZTNA Report* pane opens.
2. Click *Run Report*.
   Once the report is available, click the format to view the report in.

Others

This section lists the new features added to FortiAnalyzer for other topics relating to logging and reporting:

- Time zone settings per ADOMs/Reports on page 46

Time zone settings per ADOMs/Reports

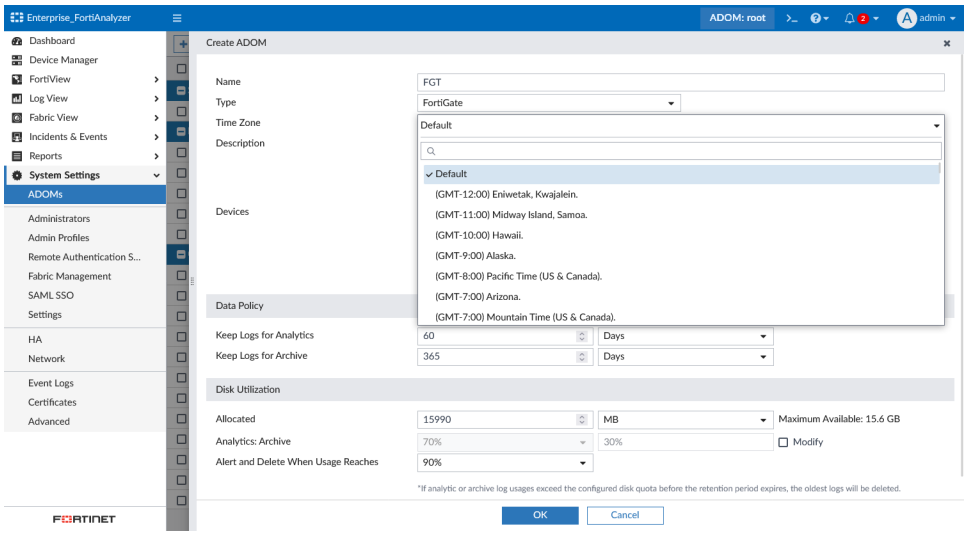
This information is also available in the FortiAnalyzer 7.4 Administration Guide:
- Creating ADOMs
- Report Settings tab

To allow a more granular reporting experience for Global deployment, different timezones can be configured on each ADOM/Report.

The *Default* time zone used for this setting is the time zone set for the FortiAnalyzer.

To configure the time zone for an ADOM:

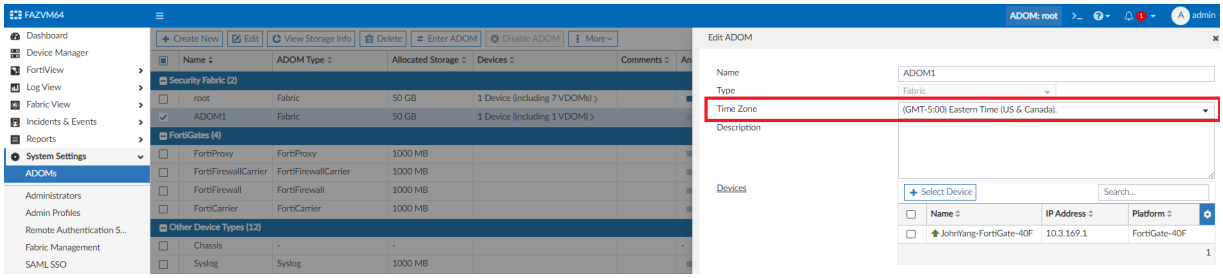
1. Go to *System Settings* > *ADOMs*.
2. Edit or create a new ADOM.
3. From the *Time Zone* dropdown, select a time zone for the ADOM.
   This time zone will be used when displaying data in *Log View* and *FortiView* for this ADOM.



4. Click *OK* to save.

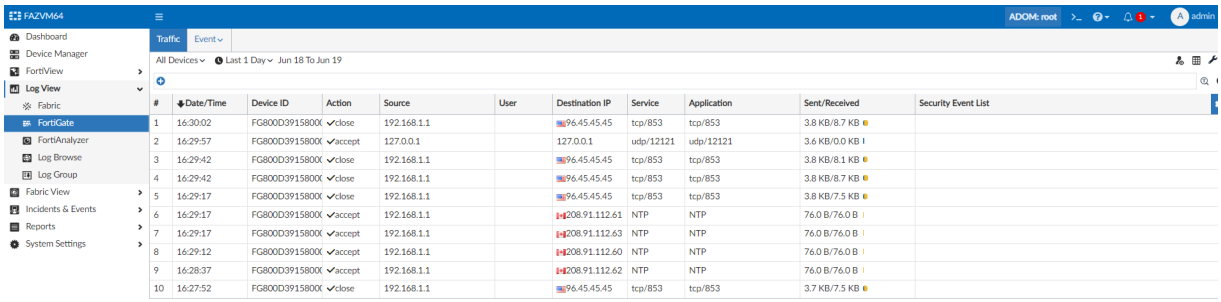
Example:

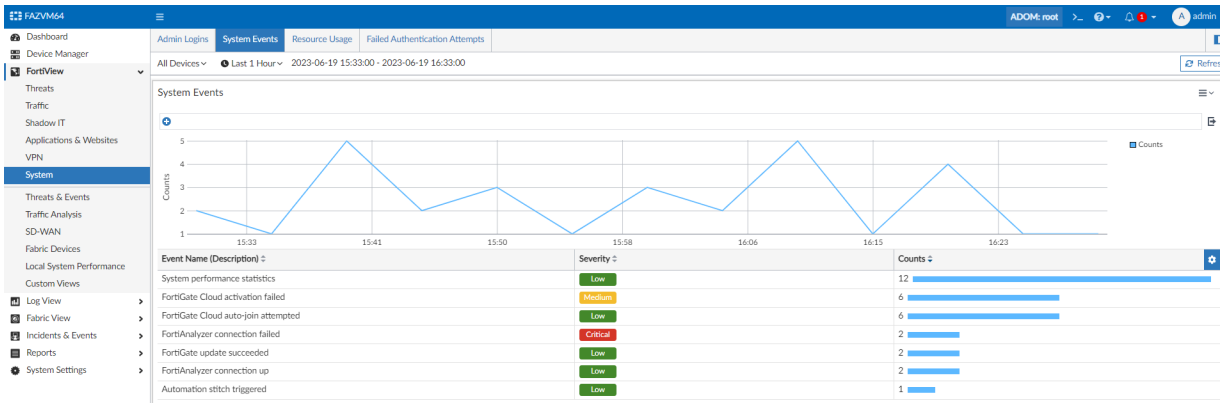
In this example, the system time zone is (GMT-8:00) Pacific Time, which is used by the root ADOM. The admin creates a new adom (ADOM1) and sets the time zone to (GMT-5:00) Eastern Time:

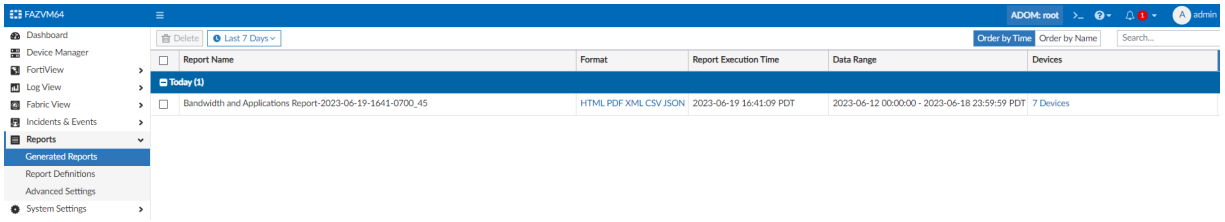


In the root ADOM, the *Log View*, *FortiView*, and *Generated Reports* panes are displayed according to the default system time zone: (GMT-8:00) Pacific Time.

For example, the admin is reviewing the panes below at approximately 16:30 Pacific Time.

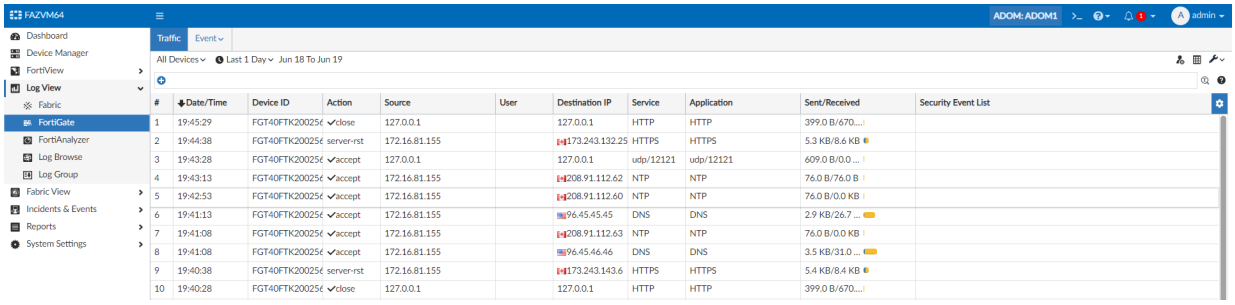


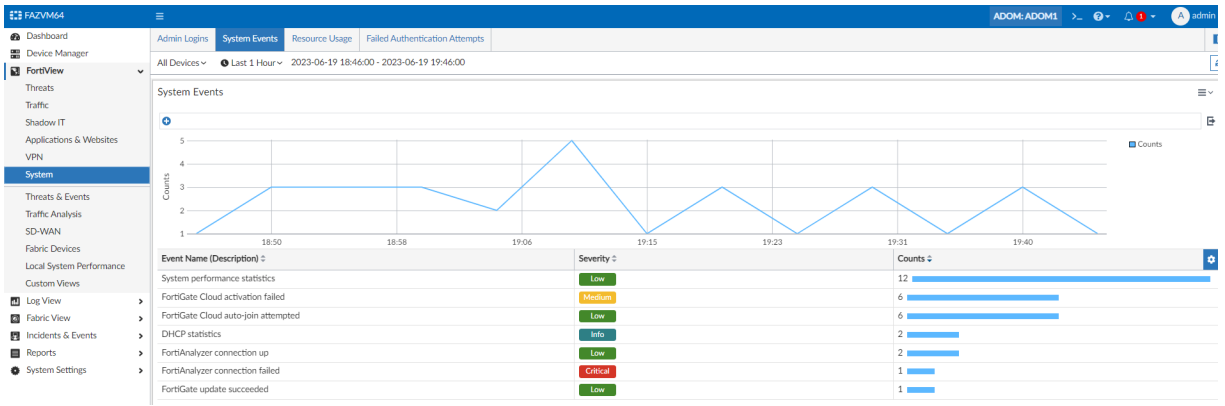


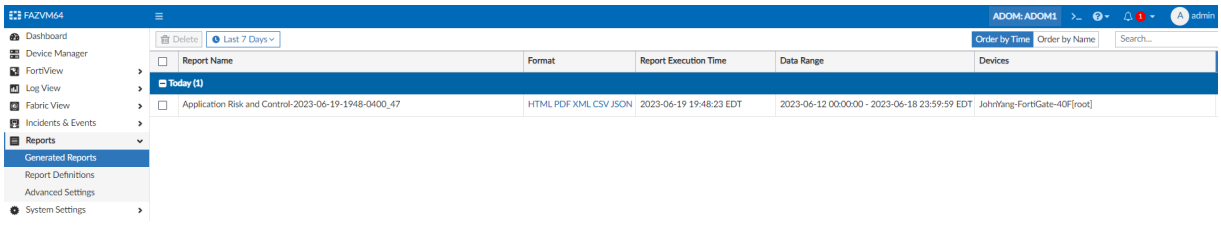


In ADOM1, the *Log View*, *FortiView*, and *Generated Reports* panes are displayed according the ADOM's specified time zone: (GMT-5:00) Eastern Time.

For example, the admin is reviewing the panes below at approximately 16:40 Pacific Time (19:40 Eastern Time).

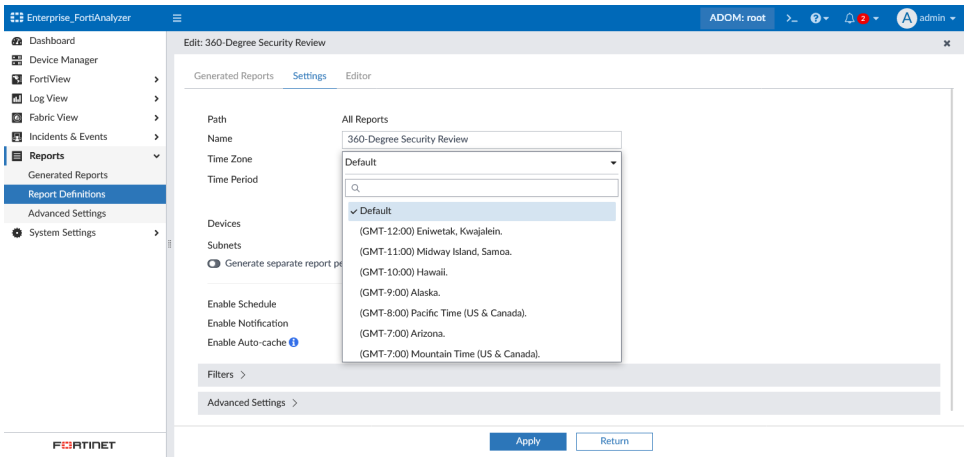






To configure the time zone for a report:

1. Go to *Reports* > *Report Definitions* > *All Reports*.
2. Double-click the report, or right-click the report and select *Edit*.
3. Go to the *Settings* tab.
4. From the *Time Zone* dropdown, select a time zone to use for data in the report output.



5. Click *Apply* to save.

System

This section lists the new features added to FortiAnalyzer for system settings:

- Others on page 50

Others

This section lists the new features added to FortiAnalyzer for other features relating to system settings:

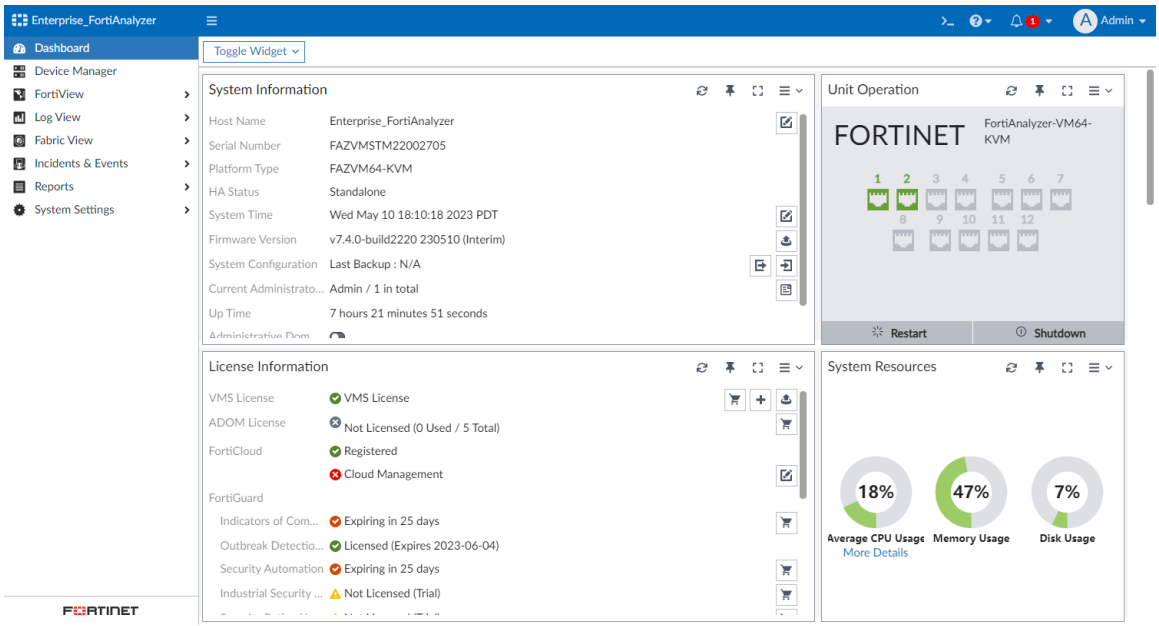
- FortiAnalyzer GUI enhancements on page 50
- Fabric of FAZ topology chart on page 54
- Fabric of FAZ: member authorization with supervisor on page 56
- Fabric of FAZ global FortiView support on page 61
- Fabric of FAZ: Central report support and creating Fabric groups on page 63
- Block out contract device from upgrading to next or major or minor release on page 66

FortiAnalyzer GUI enhancements

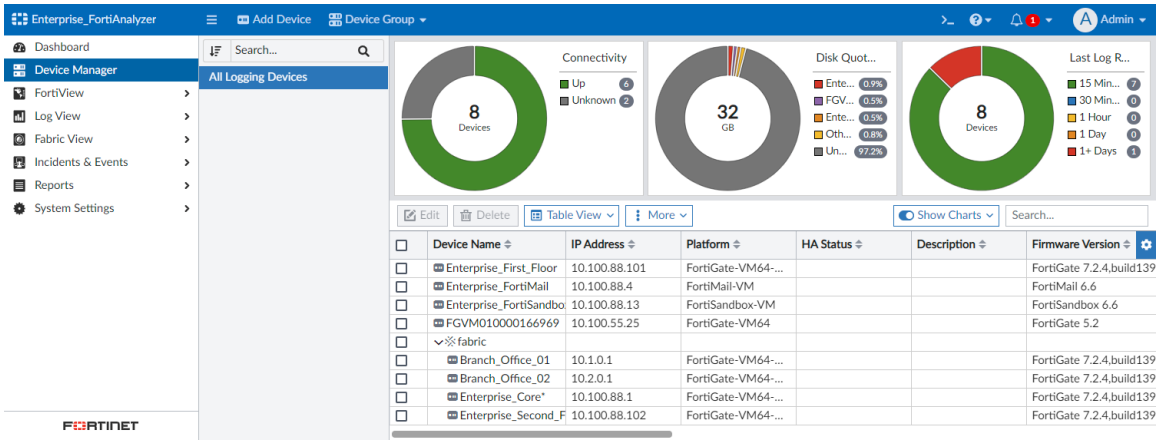
To enhance the user experience and to align to FortiOS, the following changes have been added to the FortiAnalyzer GUI:

- Uses a new and customizable landing page (*Dashboard*)
- Uses Neutrino framework
- Adopts a 3-layer navigation, making all menus accessible via a single click

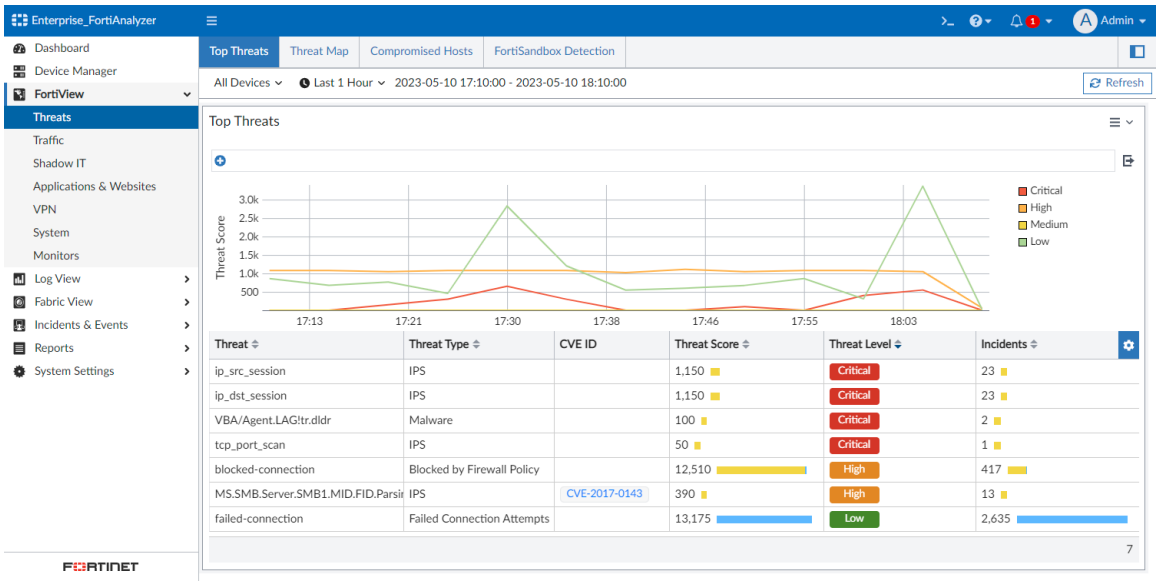
The *Dashboard* includes widgets, such as *Log Status* and *Alert Message Console*. You can toggle which widgets display from the *Toggle Widget* dropdown.



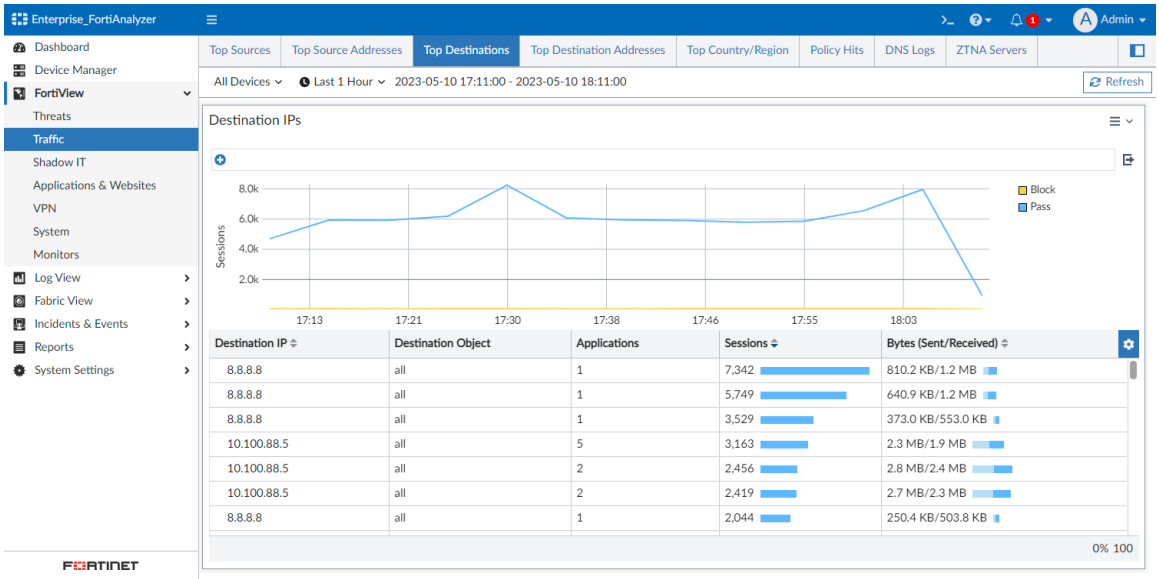
You can access other pages, such as *Device Manager*, from the left-pane navigation.



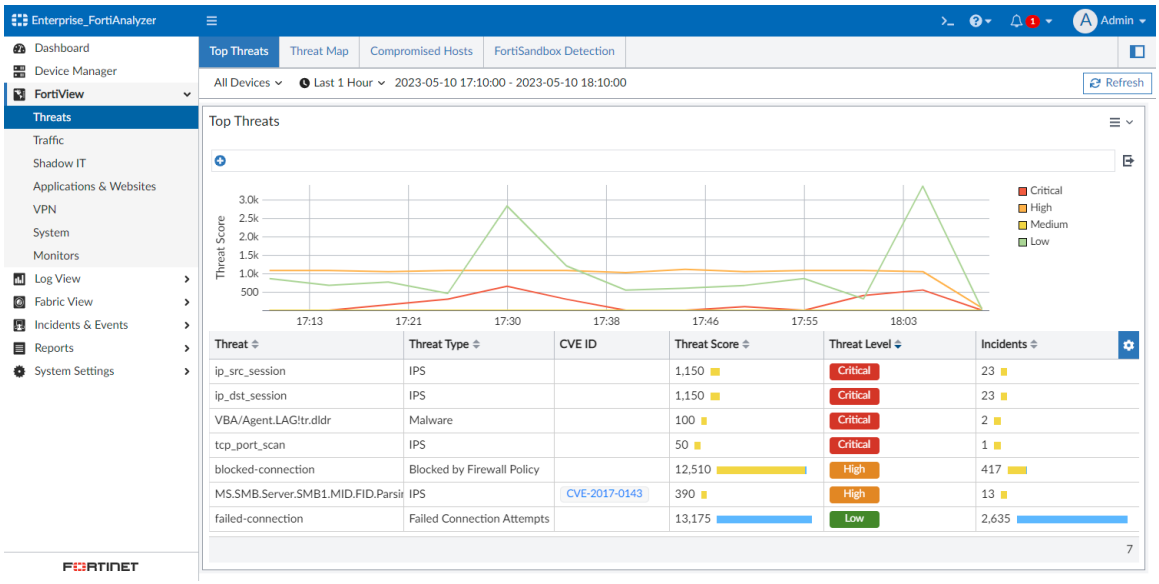
If there are sub-menus, as in *FortiView*, the left-pane navigation will expand to show other pages in that section.



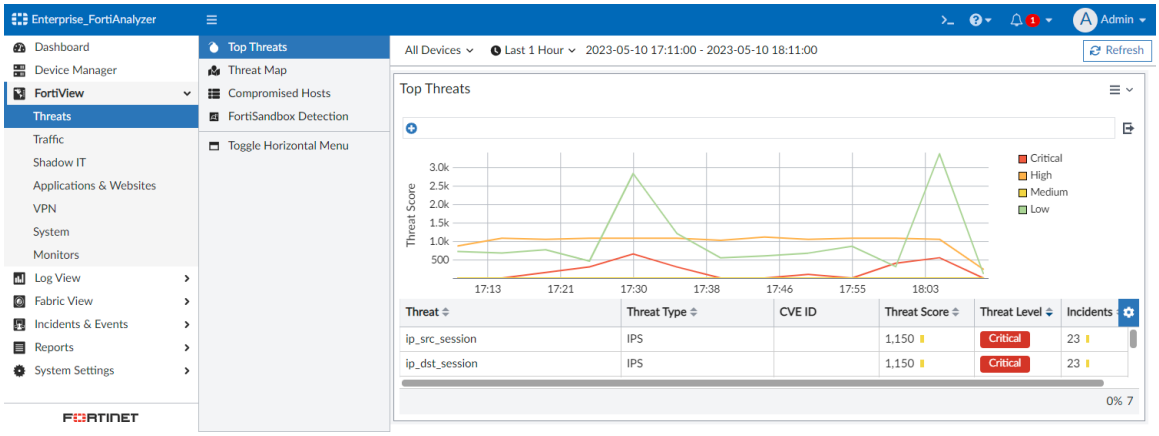
Further sub-menus may also be available along the top of the pane. For example, in the image below, the admin has navigated to *FortiView* > *Traffic* > *Top Destinations*.



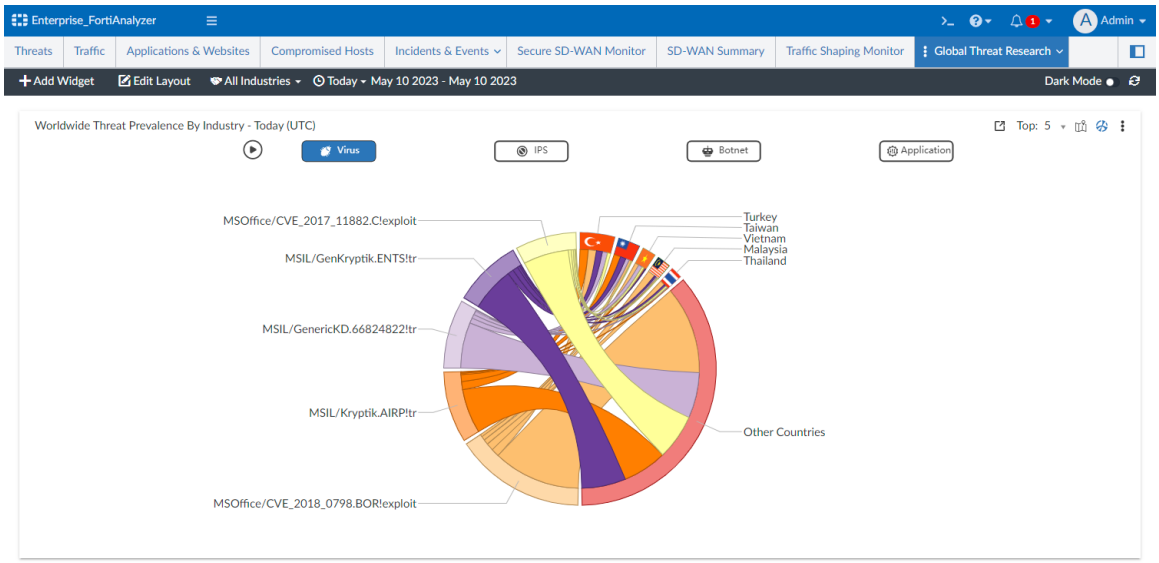
When available, you can click the horizontal view icon ( ) to switch to a vertical display of the sub-menu. The sub-menu will then display in a left-pane navigation instead.



Click *Toggle Horizontal Menu* to return to the horizontal display at the top of the pane.



On any page in the GUI, you can click the menu icon (☰) to hide the left-pane navigation. Click the menu icon (☰) again to re-open the left-pane navigation.



Fabric of FAZ topology chart

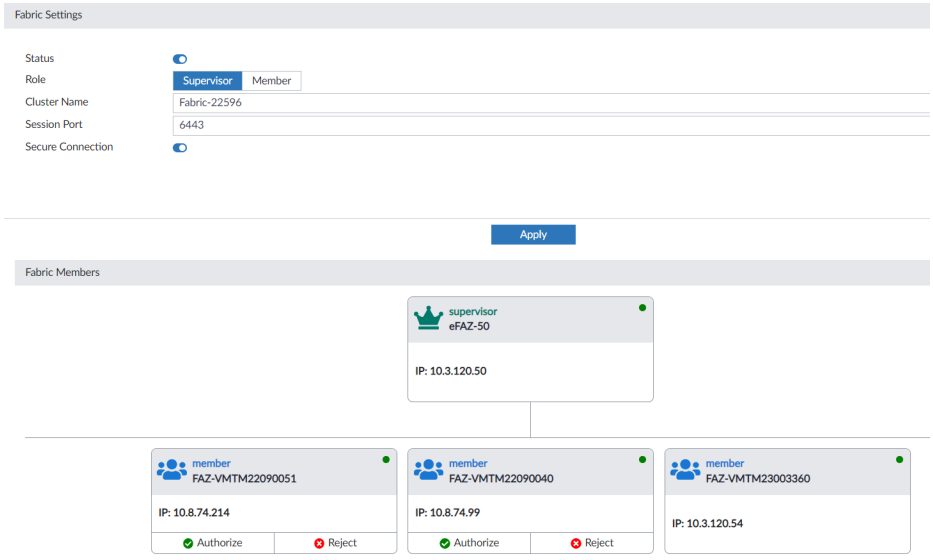
This information is also available in the FortiAnalyzer 7.4 Fabric Deployment Guide:

- Configuring the FortiAnalyzer Fabric

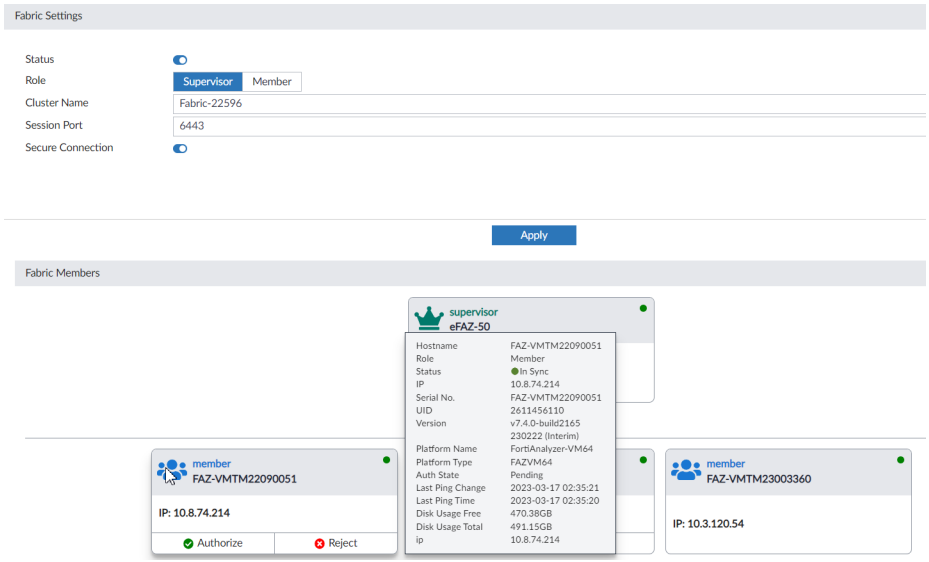
A FortiAnalyzer Fabric topology chart is displayed on the supervisor to quickly identify connected members and their corresponding status.

FortiAnalyzer Fabric supervisor:

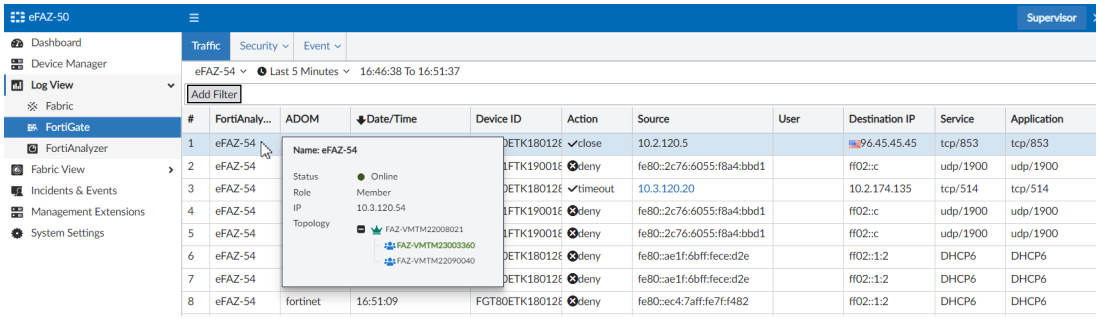
To view the topology on the supervisor, go to *System Settings* > *Fabric Management* > *Fabric Settings*. In the *Fabric Members* section, the topology displays all connected members.



You can hover over the role for a FortiAnalyzer in the topology to display more information in a tooltip.

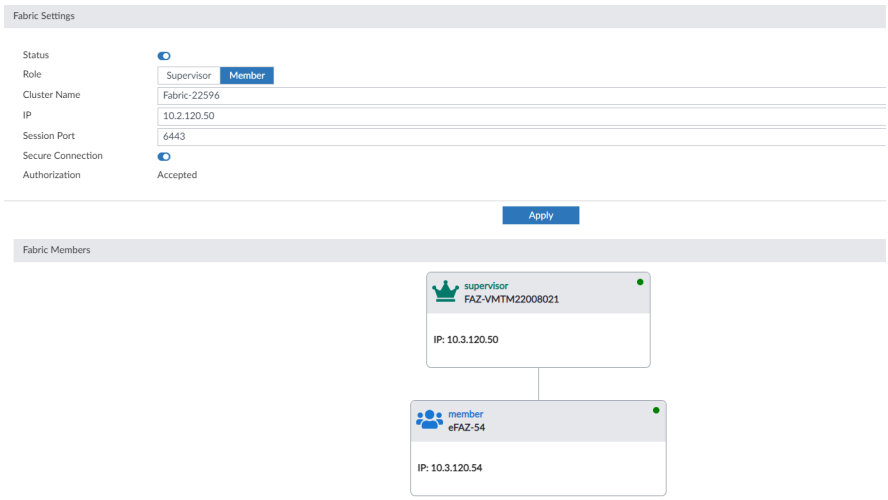


You can also see the topology in the supervisor's *Log View*. Hover over a FortiAnalyzer in the *FortiAnalyzer Host Name* column to view the topology in a tooltip.



FortiAnalyzer Fabric member:

To view the topology on a member, go to *System Settings* > *Fabric Management* > *Fabric Settings*. In the *Fabric Members* section, the topology displays only the connection to the supervisor. It does not display the other members in the FortiAnalyzer Fabric.



Fabric of FAZ: member authorization with supervisor

This information is also available in the FortiAnalyzer 7.4 Fabric Deployment Guide:

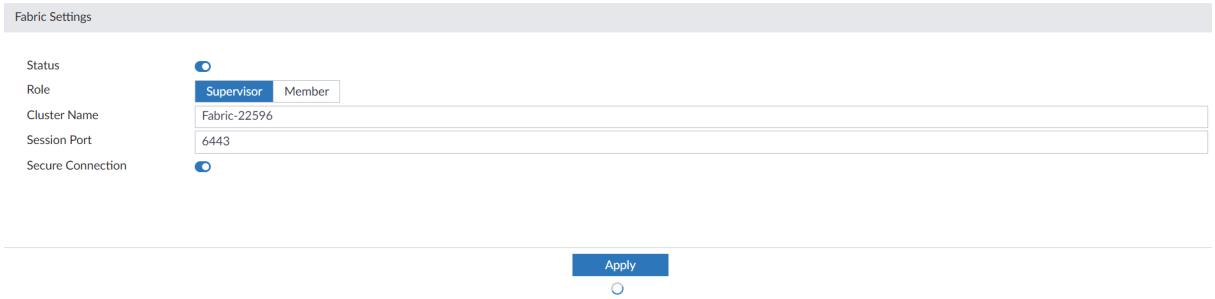
- Configuring the FortiAnalyzer Fabric

The FortiAnalyzer Fabric authentication process has been enhanced by implementing the following:

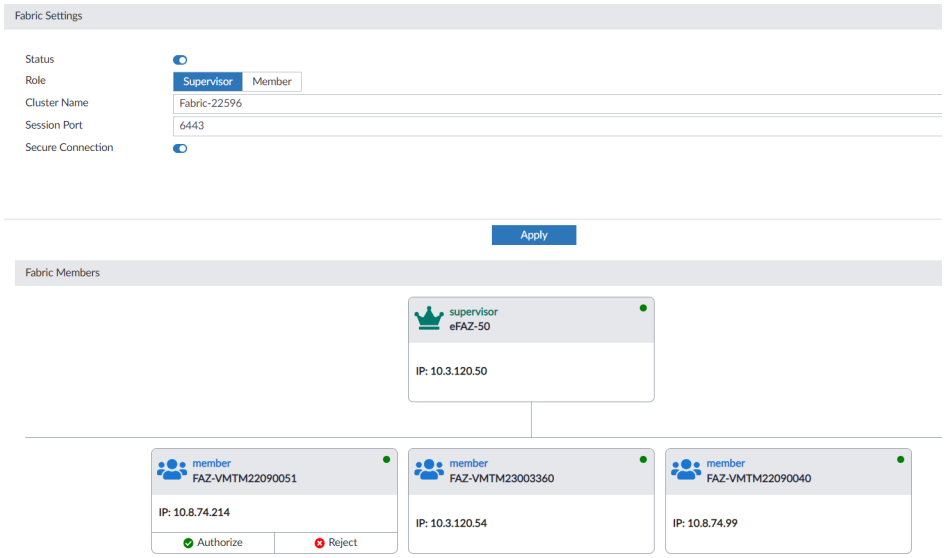
- Members can join the FortiAnalyzer Fabric by entering the cluster name and IP of the supervisor. No static password is required.
- The supervisor can authorize and reject members from joining the FortiAnalyzer Fabric.
- A `trusted-list` can be configured on the FortiAnalyzer Fabric supervisor to automatically authorize members if they match the configured serial number.
- A `trusted-list` can be configured on FortiAnalyzer Fabric members, so that they will join the FortiAnalyzer Fabric only if the supervisor matches the configured serial number.

FortiAnalyzer Fabric supervisor:

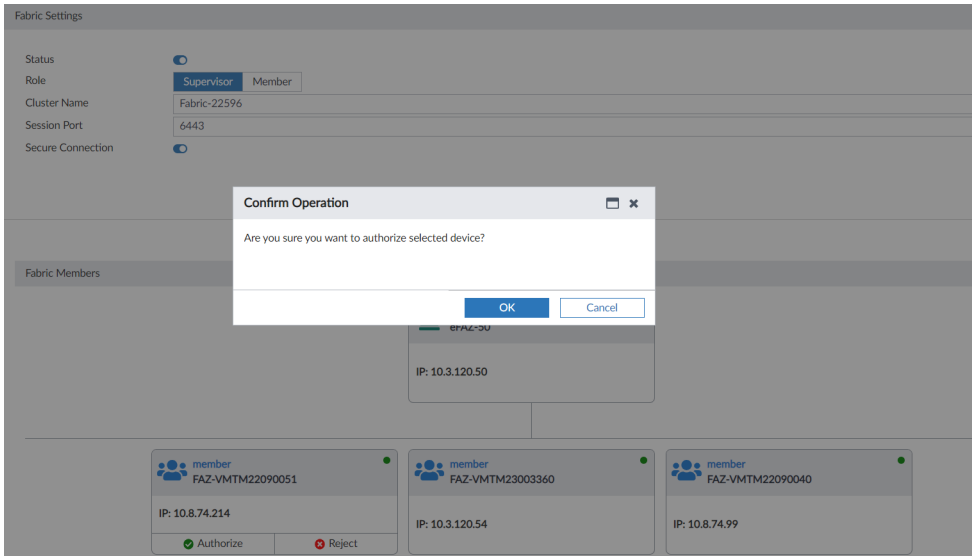
When configuring a FortiAnalyzer Fabric supervisor in *System Settings* > *Fabric Management*, there is no password configuration in the *Fabric Settings*.

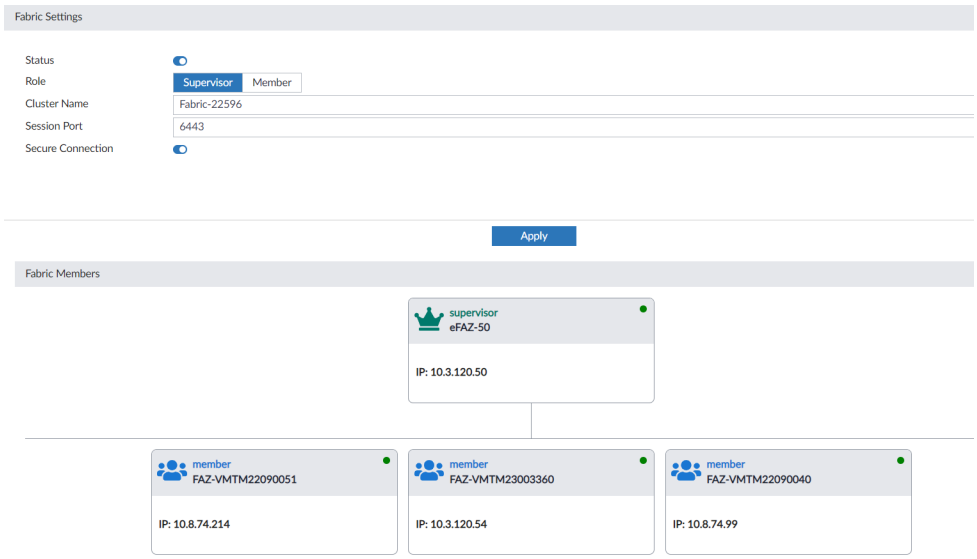


When members join the FortiAnalyzer Fabric, they will display in the topology for the supervisor. From this topology in the supervisor, you can authorize or reject the members.

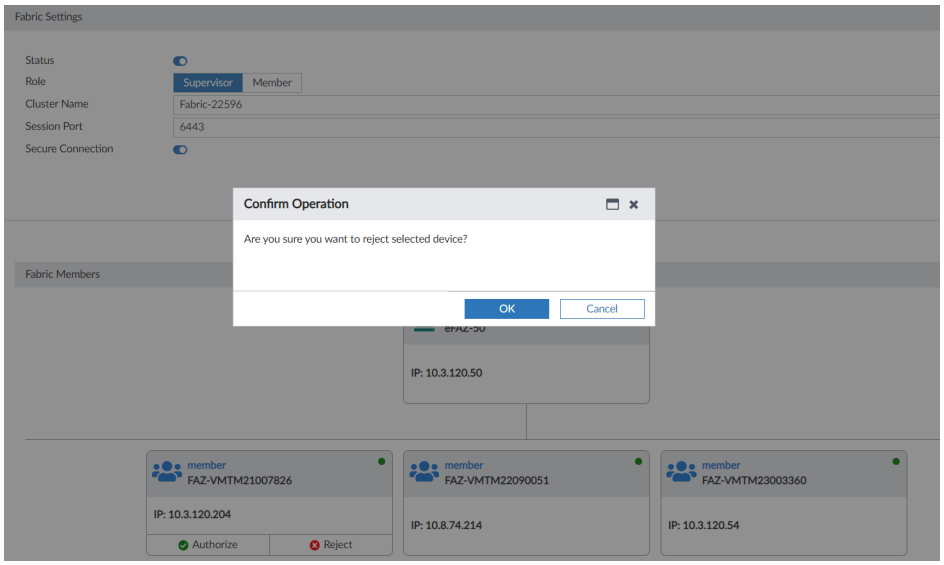


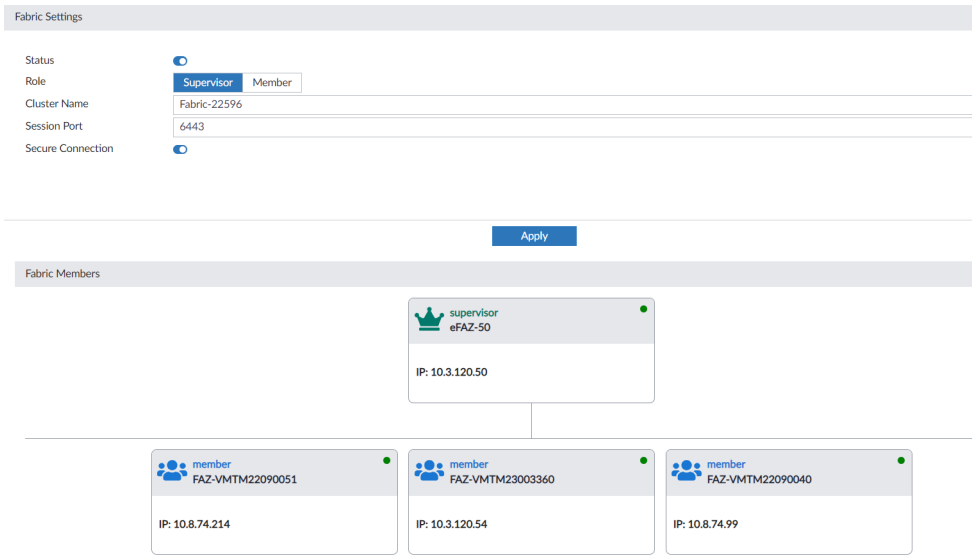
If authorized, the member will join the FortiAnalyzer Fabric and it will remain visible in the topology.





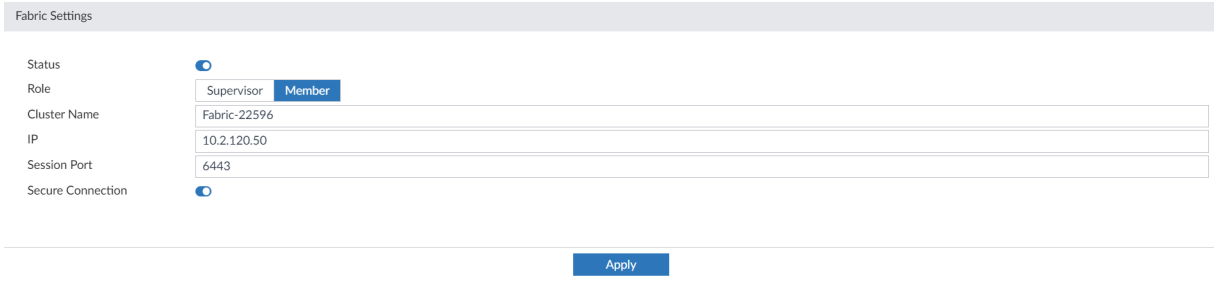
If rejected, the member will be removed from topology and it will be blocked from attempting to re-join the FortiAnalyzer Fabric for 10 minutes.



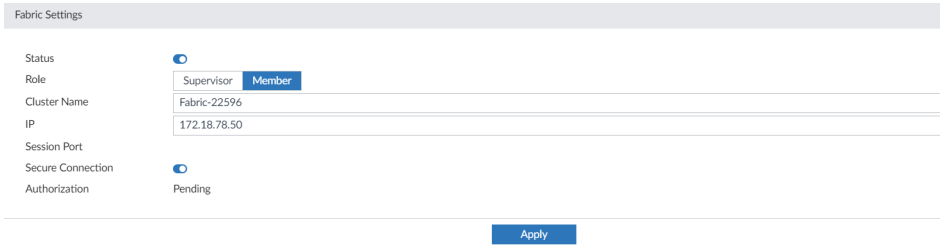


FortiAnalyzer Fabric members:

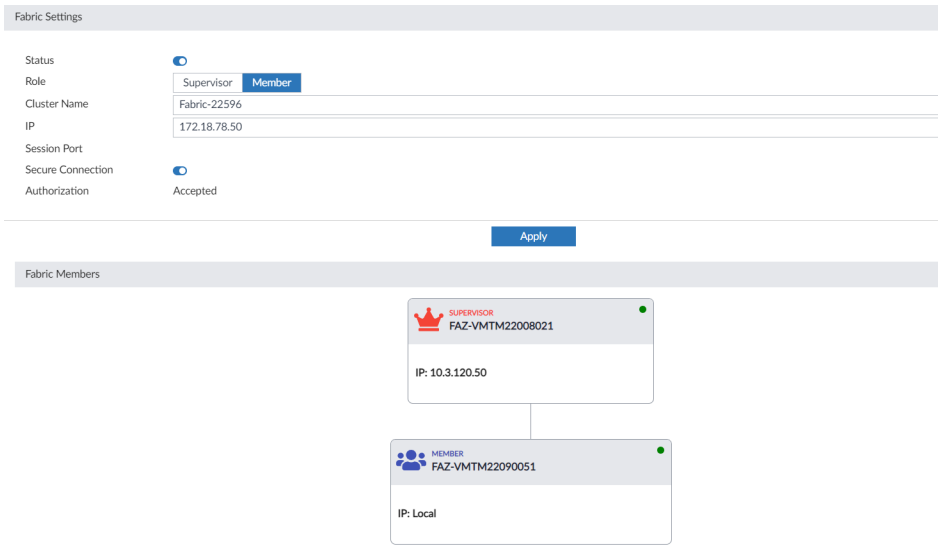
When joining a FortiAnalyzer Fabric as a member, go to *System Settings* > *Fabric Management*. You do not need to enter a password. Instead, enter the cluster name and IP of the supervisor.



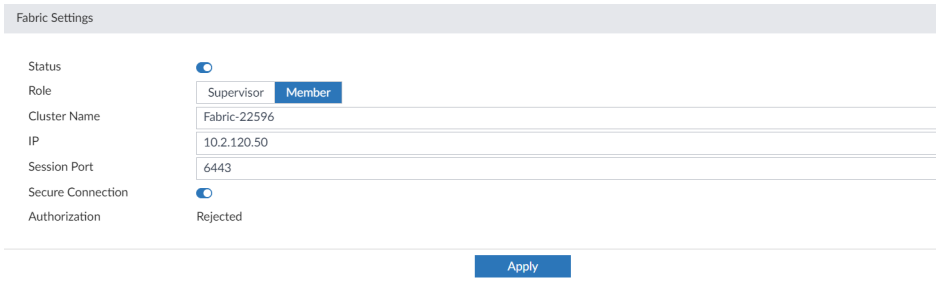
After configuring the FortiAnalyzer as a member, the *Authorization* field will display *Pending*.



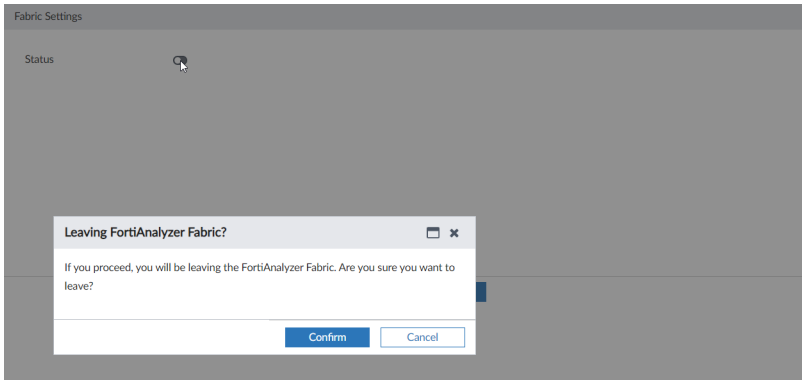
Once the member is authorized by the supervisor, the *Authorization* field will change to *Accepted*. The topology will display this member and the supervisor, but it will not display other members in the FortiAnalyzer Fabric.



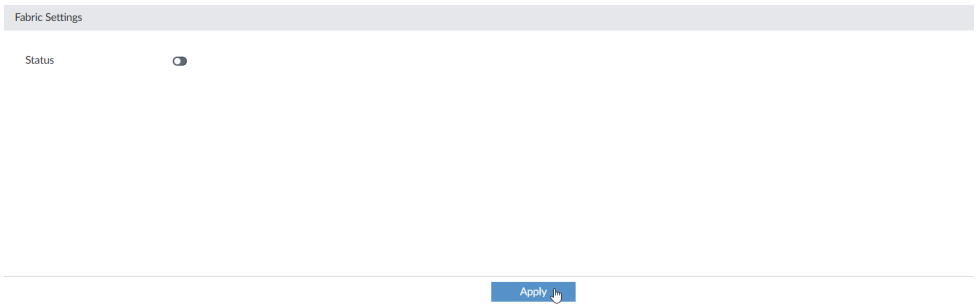
If the member is rejected by the supervisor, the *Authorization* field will change to *Rejected*. The member must wait 10 minutes before sending another request to join the FortiAnalyzer Fabric. To try again, click apply after the block-out time is complete.



To leave a FortiAnalyzer Fabric, go to *System Settings* > *Fabric Management* > *Fabric Settings* in the member and set the *Status* to disabled. A message will display to confirm the action.



After confirming the message, click *Apply* to save the configuration.



If needed, the member can re-join the FortiAnalyzer Fabric, but it will need to be authorized by the supervisor again.

Trusted-list for a FortiAnalyzer Fabric:

The `trusted-list` configuration is completed on the CLI for both the supervisor and the members.

In the supervisor's CLI, you can add members' serial numbers to a `trusted-list`. This supports wildcard; for example, FAZ-VMTM120033*. Once a member's serial number is added to the `trusted-list`, that FortiAnalyzer can automatically join the FortiAnalyzer Fabric as a member without the supervisor's authorization.

To add a member to the `trusted-list`, enter the following command in the supervisor's CLI:

```
config system soc-fabric
   config trusted-list
      edit 1
      set serial <member's serial number, which can include wildcards (*)>
   end
end
```

In the member's CLI, you can configure a `trusted-list` with the supervisor's serial number to verify the legitimacy of the supervisor. This prevents data leakage to a falsified supervisor. Members will only join the FortiAnalyzer Fabric when the supervisor's serial number matches the members `trusted-list`.

To configure a `trusted-list` on a member, enter the following command in the member's CLI:

```
config system soc-fabric
   config trusted-list
      edit 1
      set serial <Supervisor's serial number>
   end
end
```

For members without a `trusted-list` configured, they will treat all supervisors as legitimate.

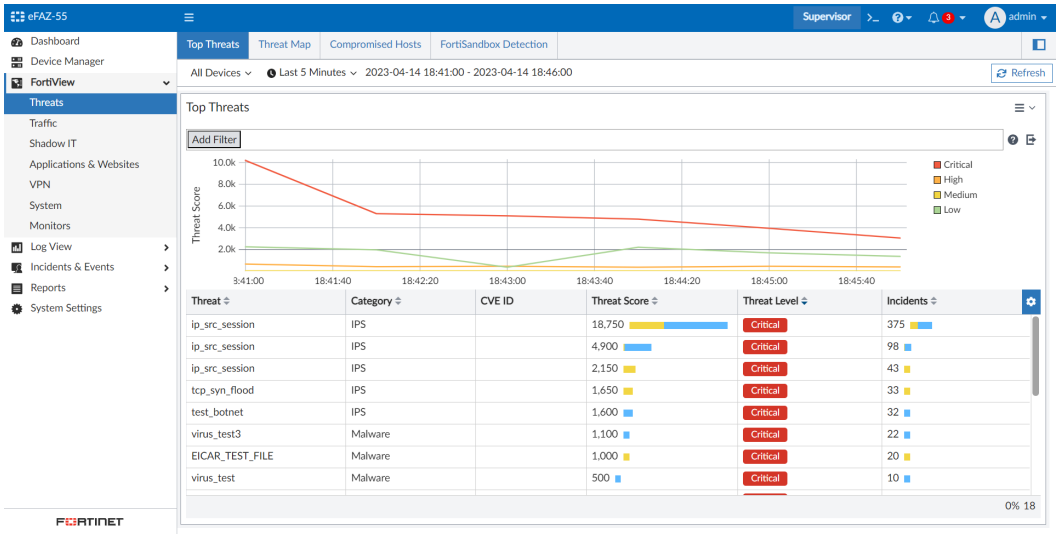
Fabric of FAZ global FortiView support

This information is also available in the FortiAnalyzer 7.4 Fabric Deployment Guide:

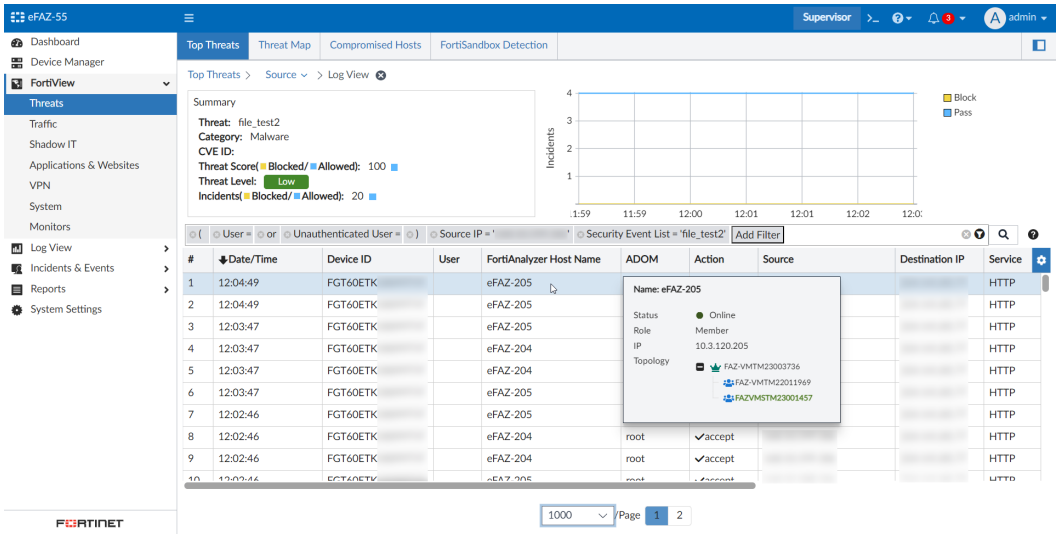
- FortiView

The FortiAnalyzer supervisor allows you to see FortiView analytics across the entire FortiAnalyzer Fabric. For more granular analysis, you can filter by the FortiAnalyzer members or ADOMs.

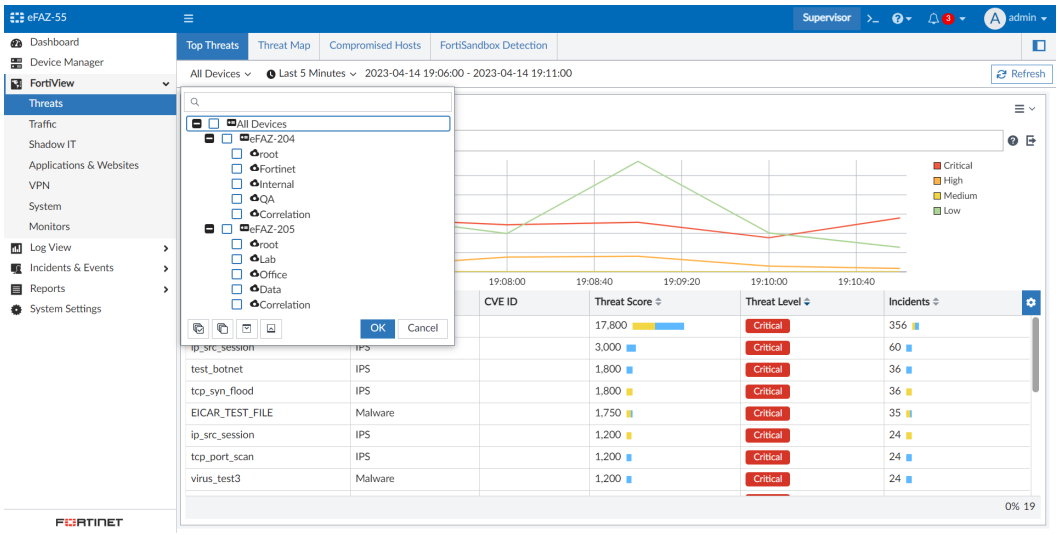
In the FortiAnalyzer Fabric supervisor, go to the *FortiView* panes. The information in these panes are generated from all members in the Fabric cluster. See the below example of *FortiView* > *Threats* > *Top Threats*.



Double-click an entry to drill down to a *Log View* of the information. In this view, you can determine the member using the *FortiAnalyzer Host Name* column.



You can also filter the *FortiView* panes by the Fabric members or ADOMs in the device list.



Fabric of FAZ: Central report support and creating Fabric groups

This information is also available in the FortiAnalyzer 7.4 Fabric Deployment Guide:

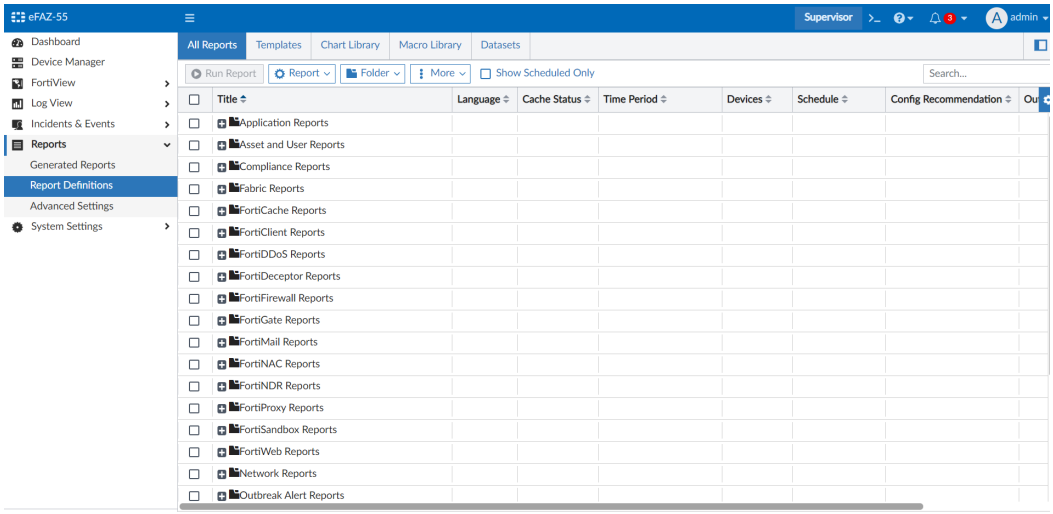
- Reports
- Fabric Groups

Reports can now be executed from the Fabric supervisor that fetches and aggregates data from multiple FortiAnalyzer Fabric members. Reports are centrally visible on the supervisor.

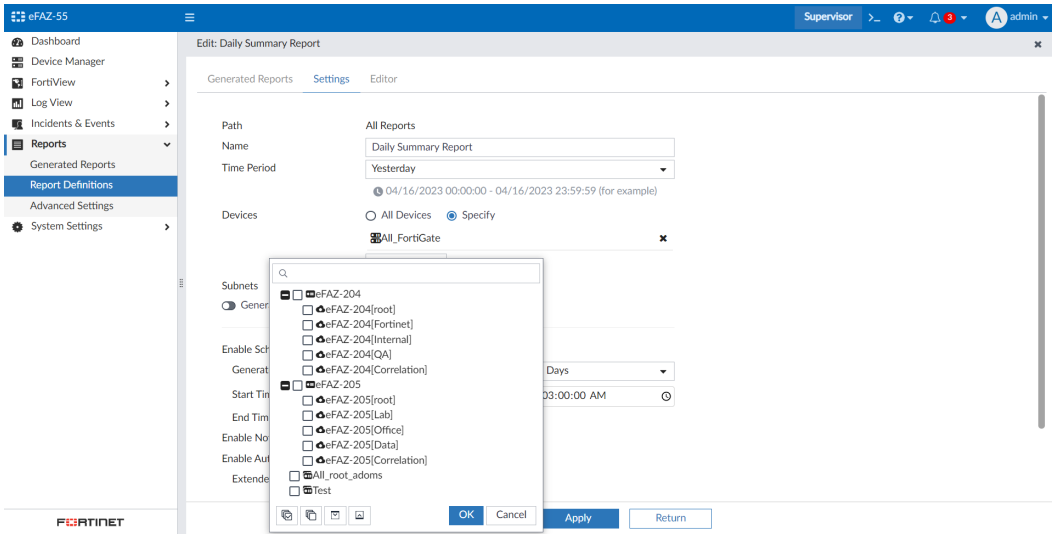
Additionally, FortiAnalyzer Fabric members or ADOMs can be grouped in a Fabric Group, which can be used in the *Log View*, *FortiView* and *Reports* device filter.

Reports:

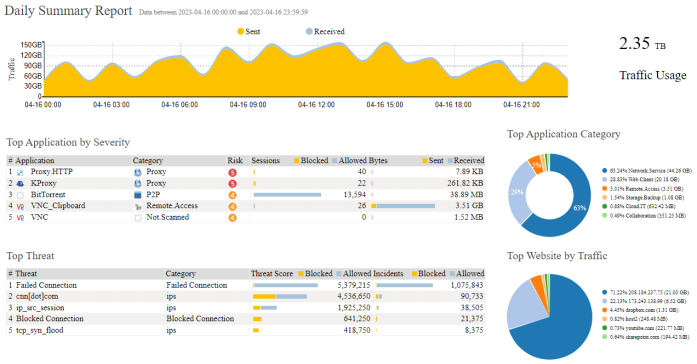
The *Reports* panes are available in the FortiAnalyzer Fabric supervisor.



In the supervisor, you can edit a report to specify which devices (Fabric members, ADOMs, and Fabric Groups) to include when running the report.

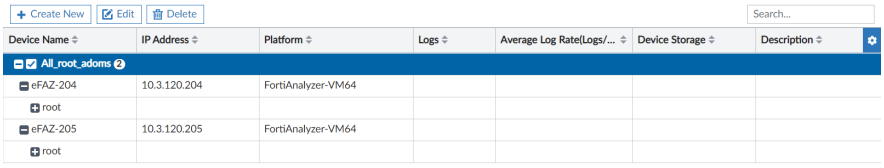


The reports' formats, charts, and tables are the same as a regular FortiAnalyzer's, but they include aggregated results from all the selected members.

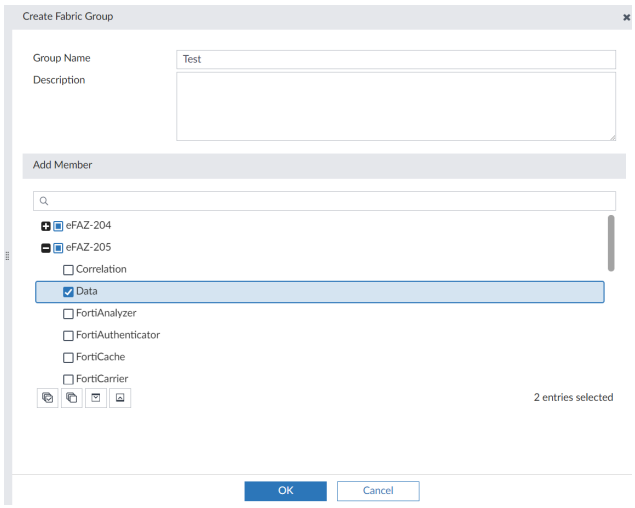


To create a Fabric Group in a FortiAnalyzer Fabric:

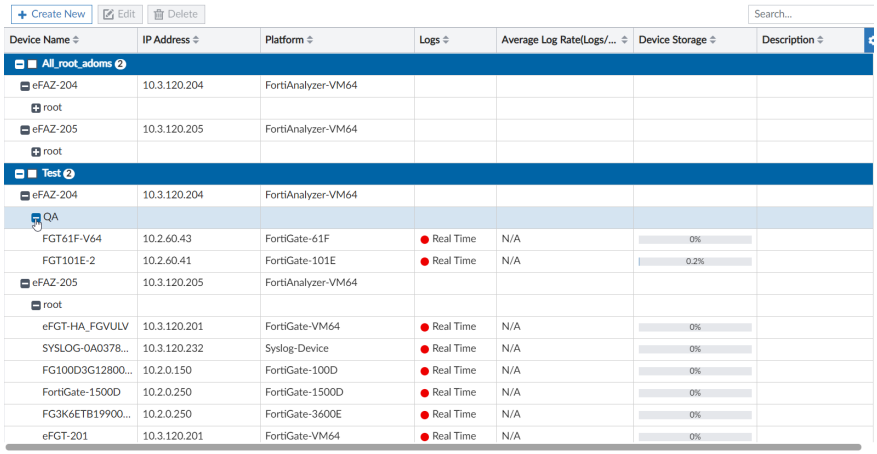
1. In the FortiAnalyzer Fabric supervisor, go to *System Settings* > *Fabric Management* > *Fabric Groups*.



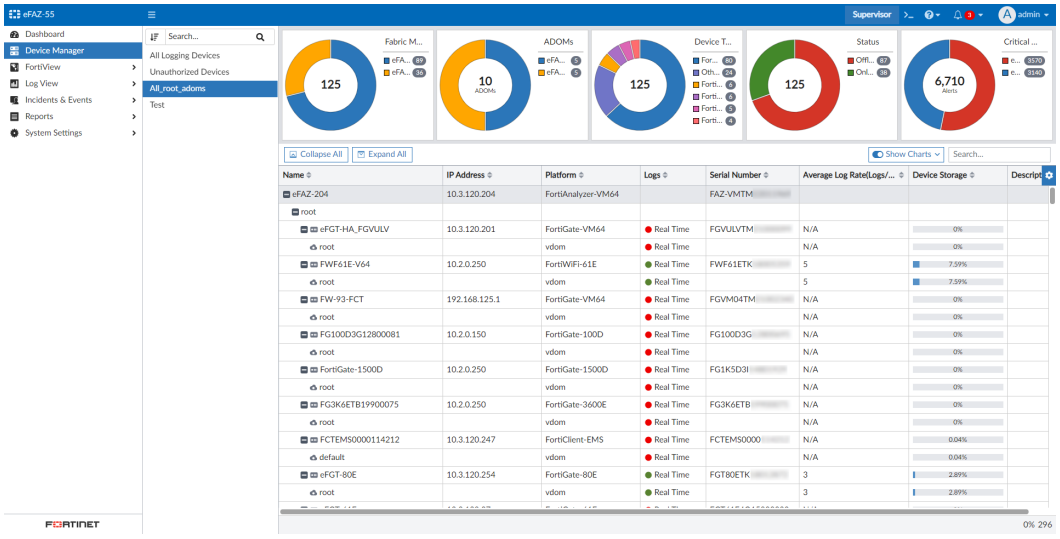
2. Click *Create New*.
3. In the *Group Name* field, enter a name for the Fabric Group.
4. In the *Add Member* section, select the FortiAnalyzer Fabric members to include.
   To add only specific ADOMs from the member, expand the member in the list and select the ADOMs to include.



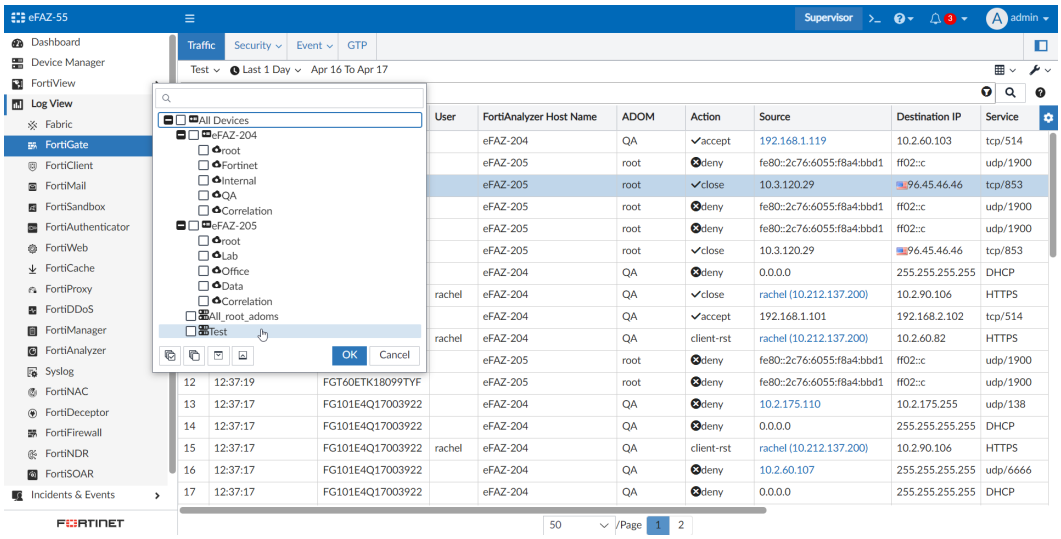
5. Click *OK*.
   The Fabric Group can now be edited or deleted from the table.



The Fabric Group is also visible in *Device Manager*.



It can be selected in the device filter for *FortiView*, *Log View*, and *Reports*. See an example in *Log View* below.



Block out contract device from upgrading to next or major or minor release

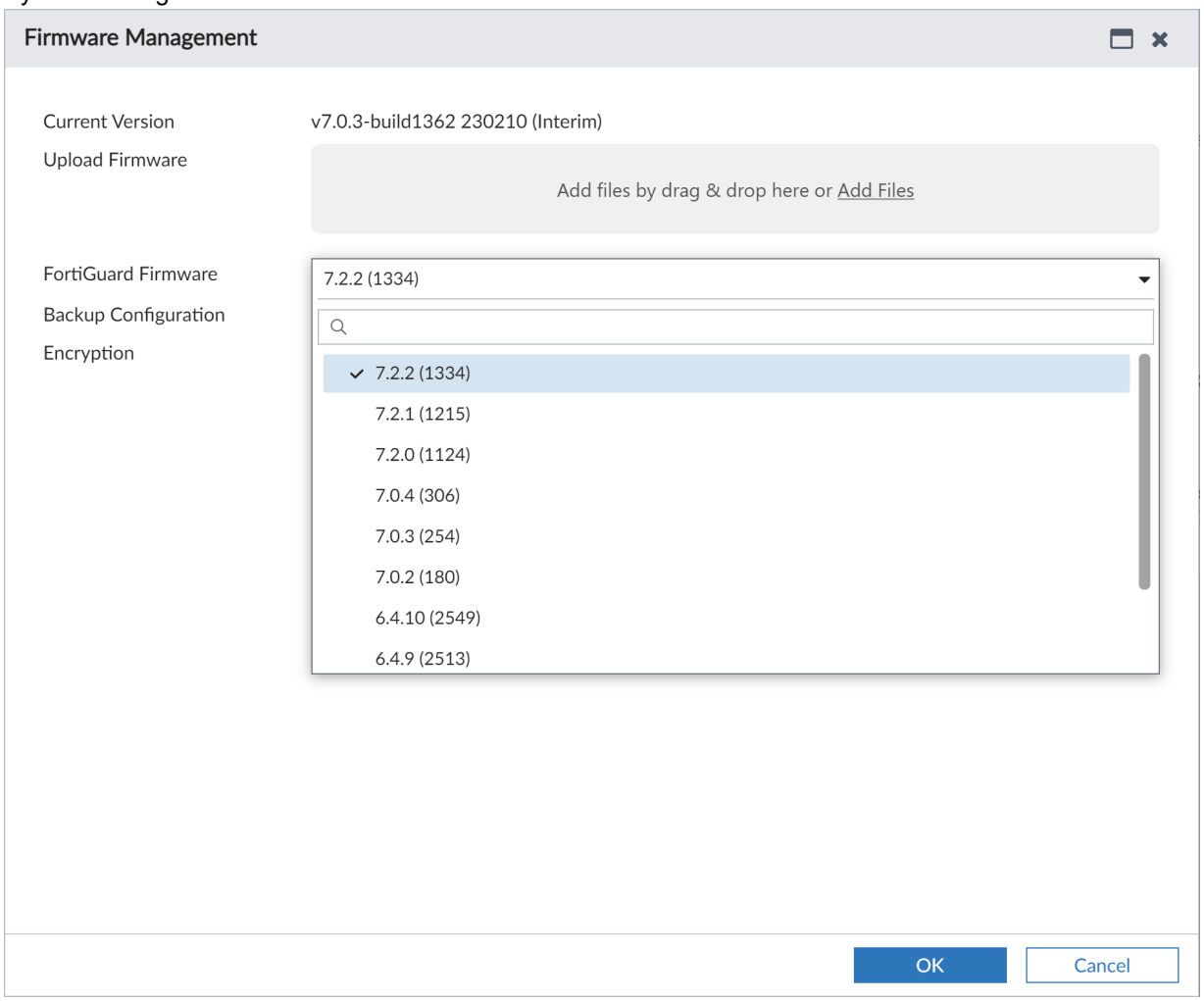
This information is also available in the FortiAnalyzer 7.4 Administration Guide:

- Updating the system firmware.
- Updating the system firmware

To view available FortiGuard images:

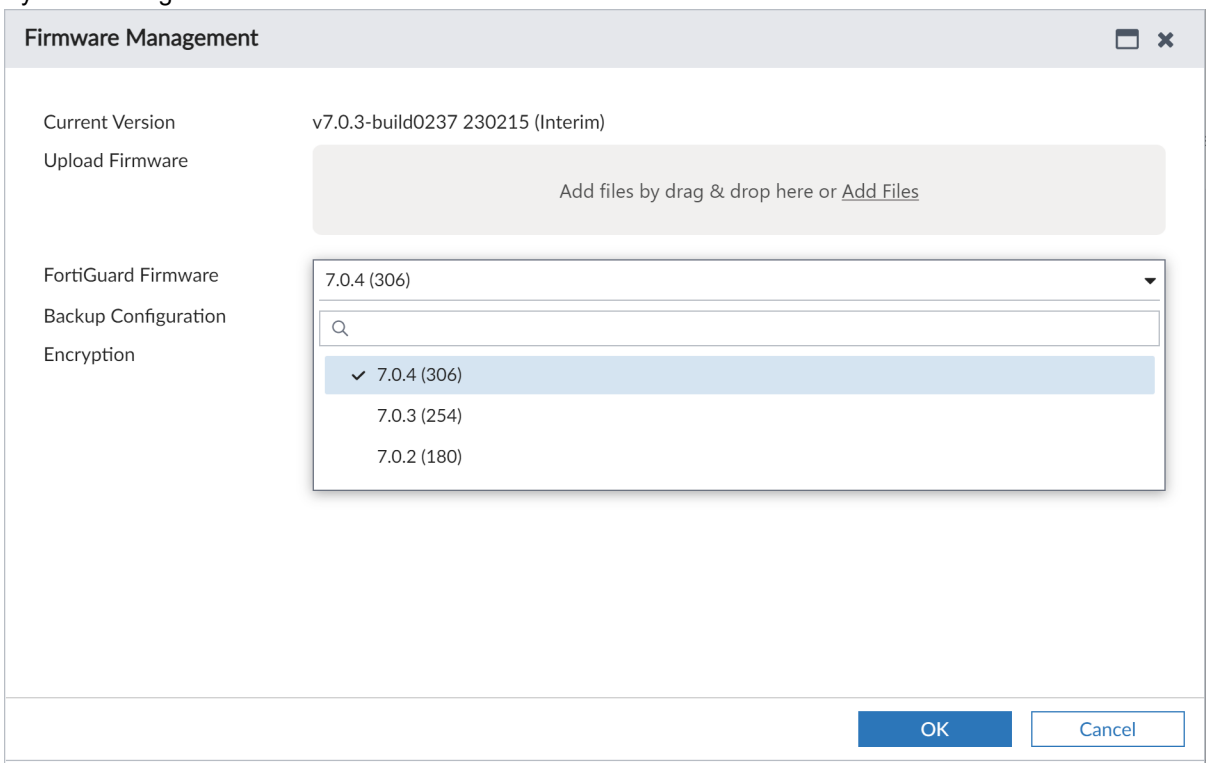
1. A FortiAnalyzer with a valid contract will display all available FortiGuard images and allow upgrading or downgrading to any version.

- System Settings:

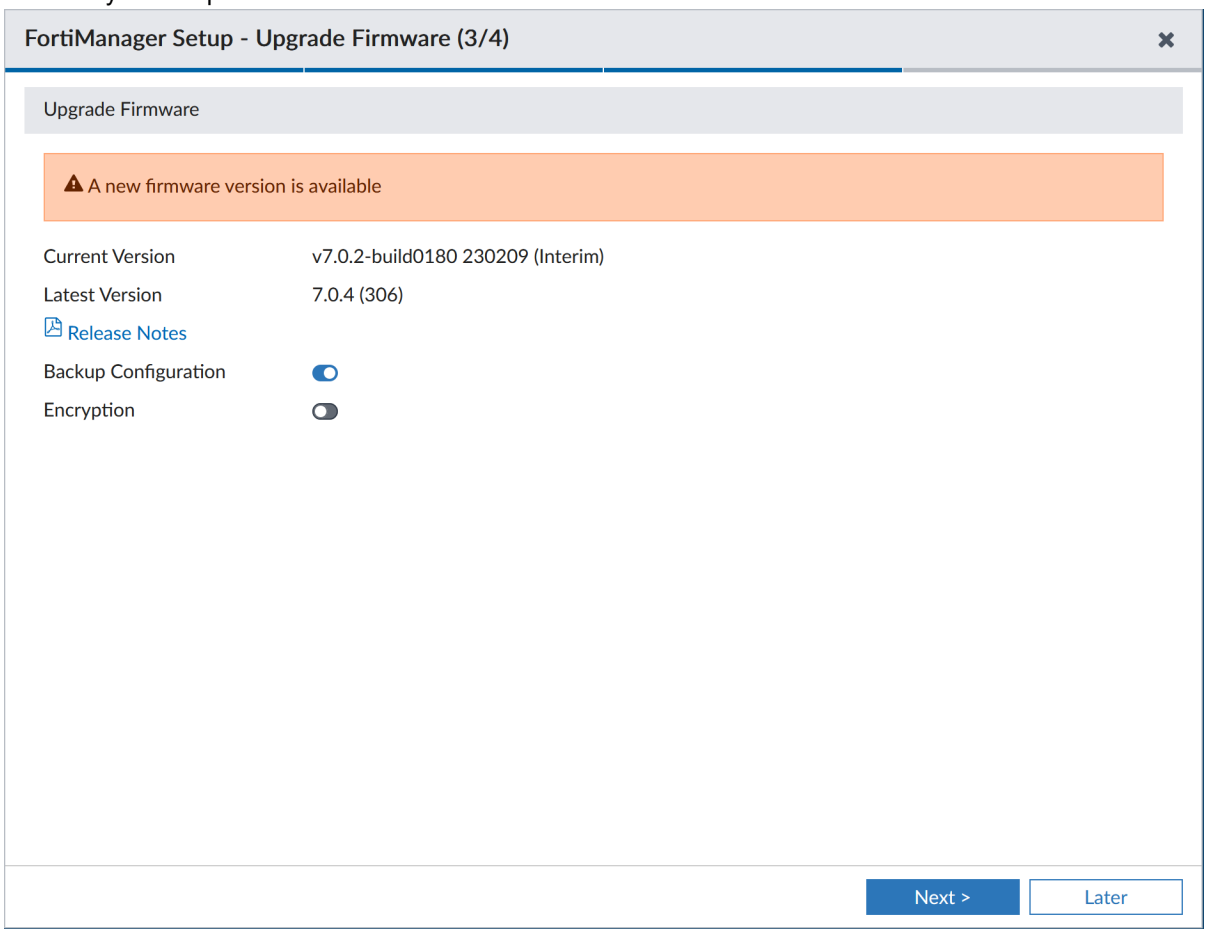


2. A FortiAnalyzer without a valid contract or with an expired contract will only display available patch images and support patch upgrades.

- System Settings:



- FortiAnalyzer setup wizard:



Cloud Services

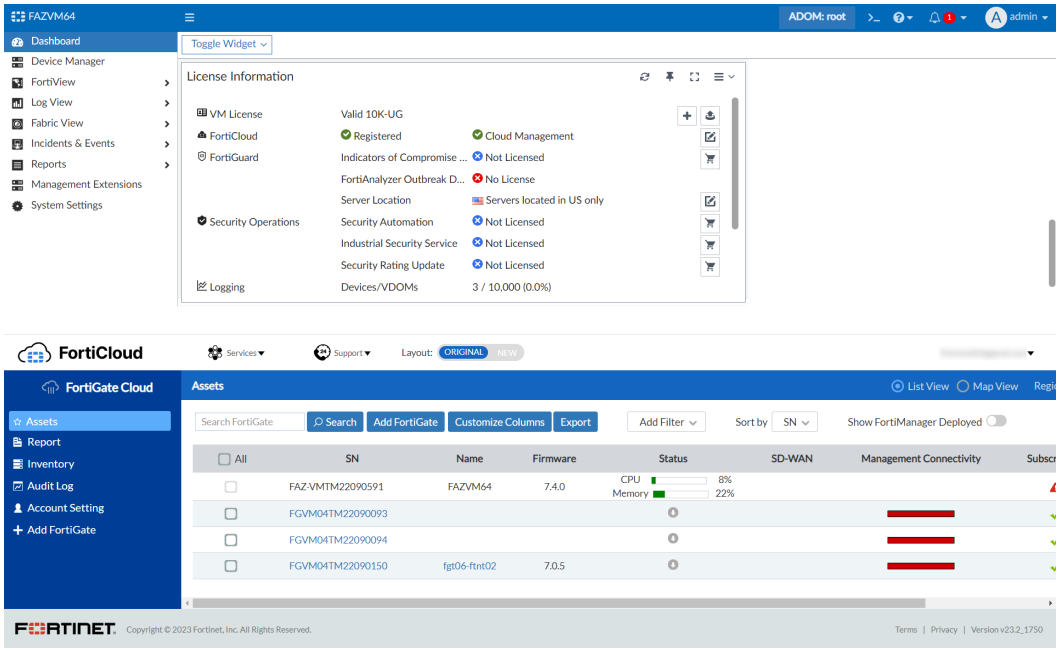
This section lists the new features added to FortiAnalyzer for cloud services:

- FortiAnalyzer supports FortiCare Elite Service on page 70

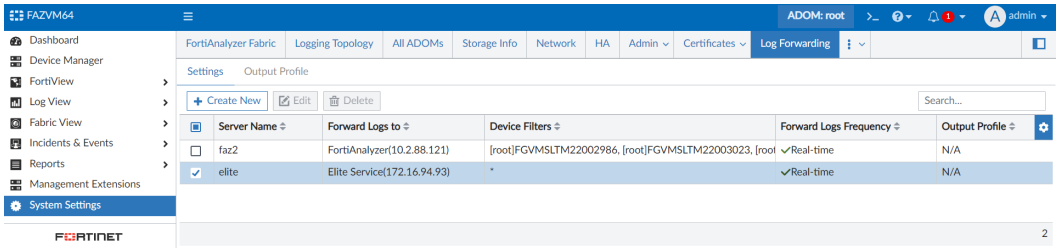
FortiAnalyzer supports FortiCare Elite Service

FortiAnalyzer and FortiAnalyzer Cloud now supports FortiCare Elite Service.

To use this service, cloud management must be enabled on the FortiAnalyzer and the FortiGate Cloud portal.



Log forwarding configuration to the Elite Service can be viewed in the FortiAnalyzer GUI. This log forwarding configuration cannot be edited or deleted.



The log forward configuration to Elite Service is also visible in the FortiAnalyzer CLI. For example:

```
config system log-forward
   edit 40000
      set mode forwarding
         set fwd-max-delay realtime
```

```
        set server-name "elite"
        set server-addr "172.16.94.93"
        set fwd-server-type elite-service
        set fwd-reliable enable
        set fwd-compression enable
        set fwd-archives disable
        set proxy-service disable
           config device-filter
              edit 1
                 set action include-like
                 set device "*"
              next
           end
        set log-filter-status enable
           config log-filter
              edit 1
                 set field level
                 set oper >=
                 set value "critical"
              next
              edit 2
                 set field logid
                 set value "0110052000"
              next
           end
        set signature 1449934396
     next
```

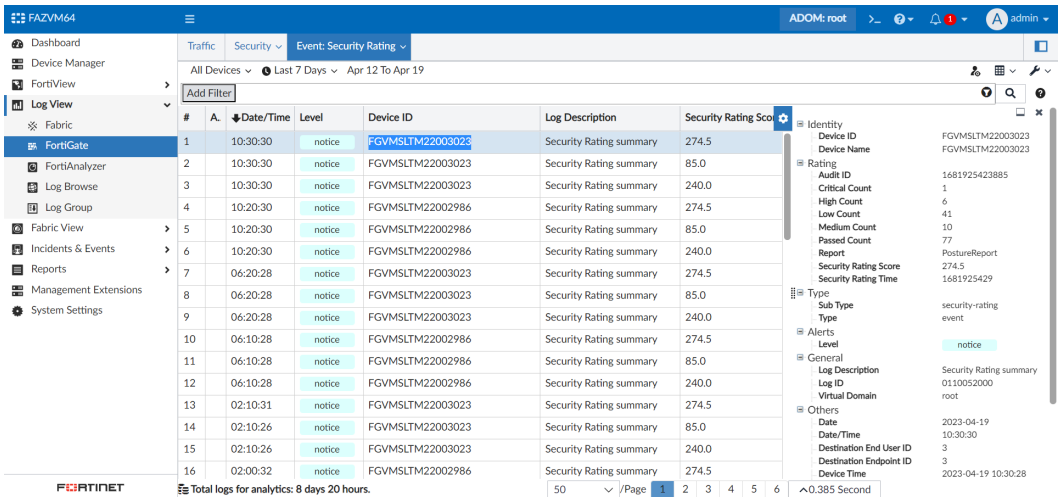
You can disable the Elite Service in the FortiAnalyzer CLI, if needed. It can also be re-enabled using the same command. In the FortiAnalyzer CLI, enter:

```
config system central-management
   set elite-service {enable | disable}
end
```

If `elite-service` is disabled, the log forwarding to Elite Service will automatically be removed. FGC will push the configuration back if the `elite-service` is later set to `enable`.

```
FAZVM64 # config system central-management
   (central-management)# get
   type  : cloud-management
   elite-service  : enable
```

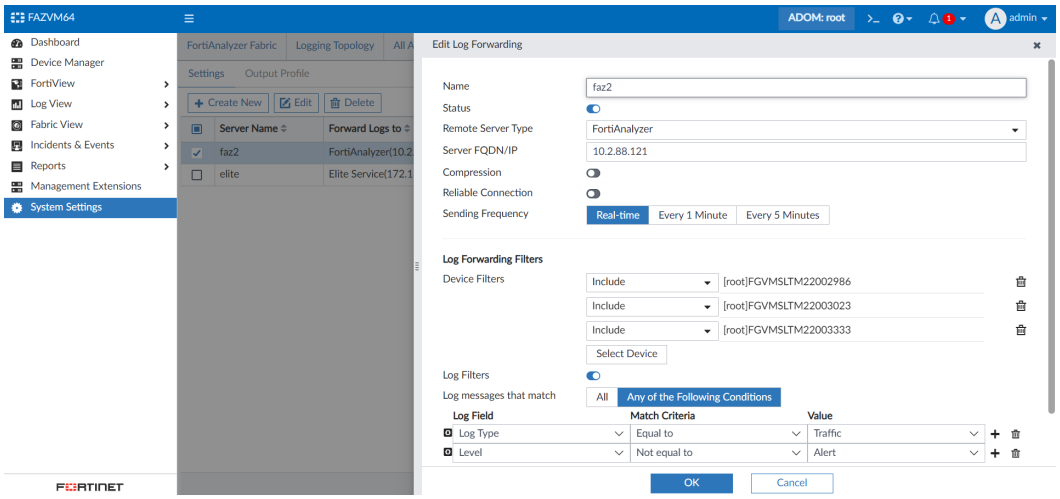
Logs that meet the filter within the log forward configuration will be forwarded to Elite log server. See a sample log in the FortiAnalyzer GUI below:



Sample logs from Elite log server:

```
2023-04-14 13:50:42,136 DEBUG Processing /dev/shm/fams/log_upload/proc/FAZ-
     VMTM22090591.1264692.nrt.e.1681505055.562204.34406
2023-04-14 13:50:42,137 DEBUG Create new raw log file: elog_20230414_135042 for (*****,
     elog)
2023-04-14 13:50:47,083 DEBUG ---sending elite kafka msg---,
     elitelogserver.remoteaccessmgr.faz.fsbp, {"action":"downloadFsbpFile","data":
     {"fazSn":"FAZ-
     VMTM22090591","fgtSn":"FGVMSLTM22002986","auditId":*****,"accountId":*****,"auditTime"
     :1681490426}}
```

Note that this log forward configuration does NOT impact other types of log forwarding.



The Elite log server can call API to get the Fortinet Security Best Practices (FSBP) reports.

API:

```
{
   "apiver": 3,
   "url": "/fazsys/auditrpt/fgt-orig-rpt",
   "data":
      {
         "devid": "FGVMSLTM22002986",
         "auditID": "1681505424727"
```

```
        }
    }
```

The reports are updated in FortiAnalyzer:

```
bash# cd /drive0/private/restapi/audit_rpt/
bash# ls
FGVMSLTM22002986                    FGVMSLTM22002986_PostureReport      FGVMSLTM22003023_OptimizationReport
FGVMSLTM22002986_CoverageReport     FGVMSLTM22003023                    FGVMSLTM22003023_PostureReport
FGVMSLTM22002986_OptimizationReport FGVMSLTM22003023_CoverageReport
bash#
```

This log forward config does not impact other types of log forward in FortiAnalyzer.

Operational Technology

This section lists the new features added to FortiAnalyzer for Operational Technology:

- Operational Technology (OT) Security Service on page 74
- OT Purdue Model in a consolidated Asset & Identity Center Dashboard on page 76
- OT Security Risk Report on page 79

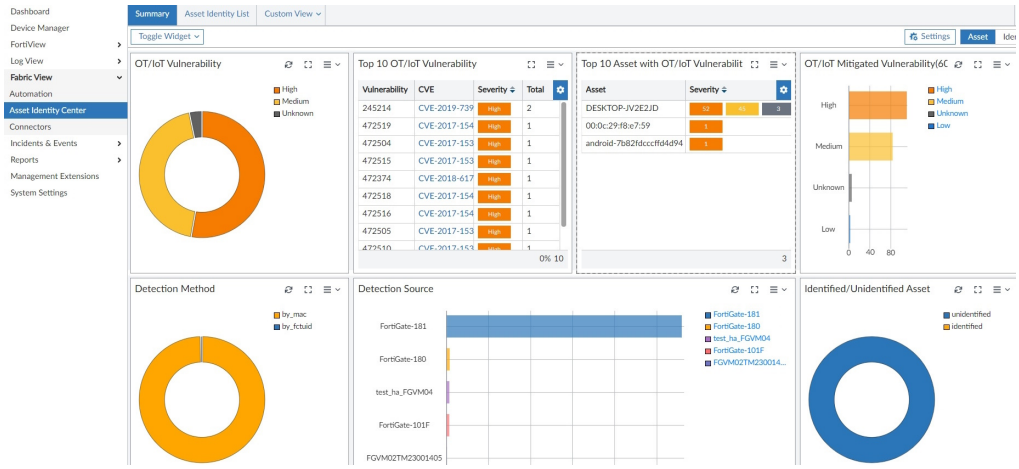
Operational Technology (OT) Security Service

Upon purchasing the OT Security Service Entitlement, the *Asset Identity Center* in FortiAnalyzer will include valuable information regarding the detected OT/IoT vulnerabilities. This includes information such as:

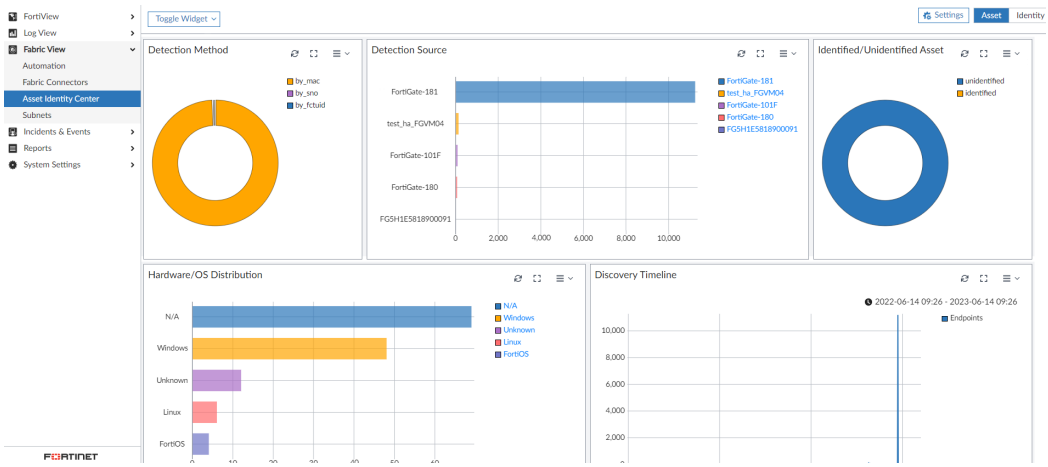
- A breakdown of OT/IoT vulnerabilities with corresponding severity
- Top 10 OT/IoT vulnerabilities by number of occurrences
- Top 10 assets with OT/IoT vulnerabilities
- Details of the vulnerabilities per endpoints

With this service, you can access the following features:

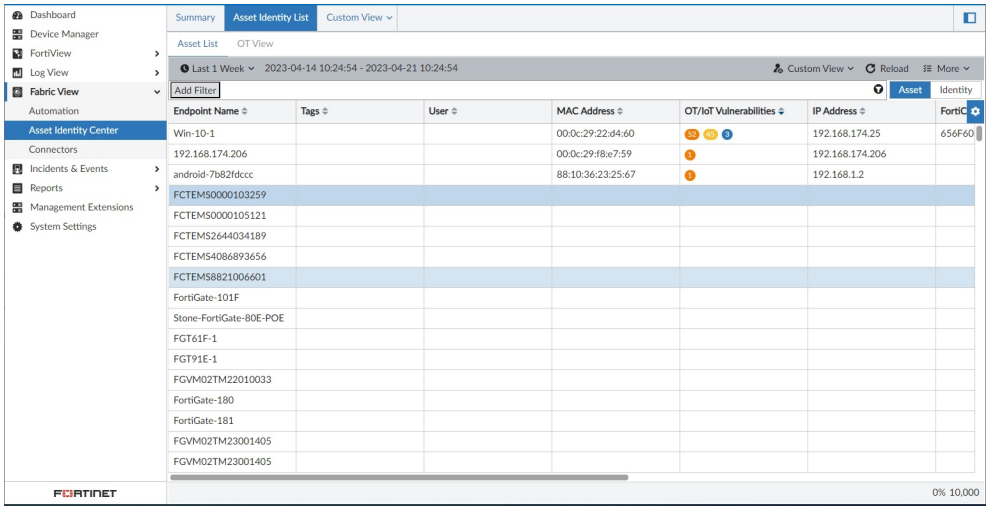
- Go to *Asset Identity Center* > *Summary* for OT/IoT Vulnerability widgets.



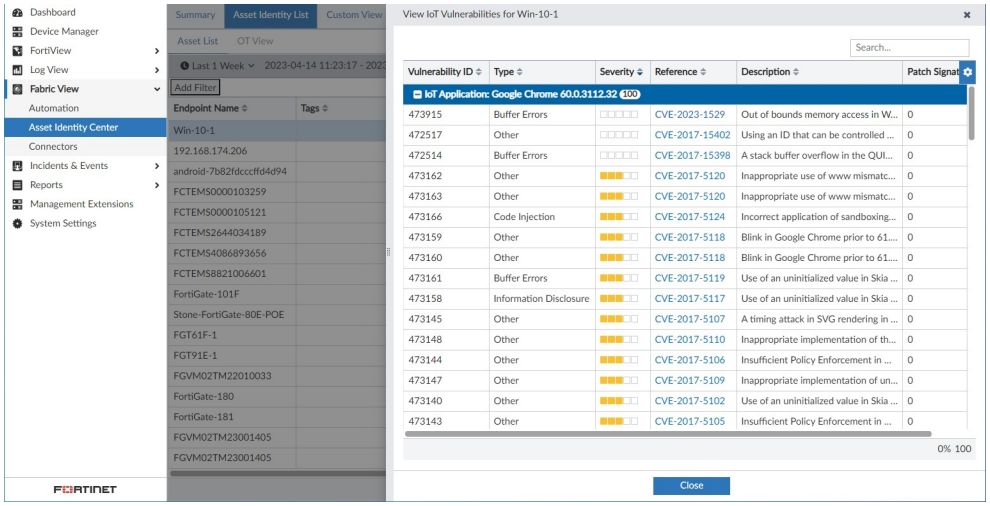
If you do not have a license for the service, the widgets will not be visible.



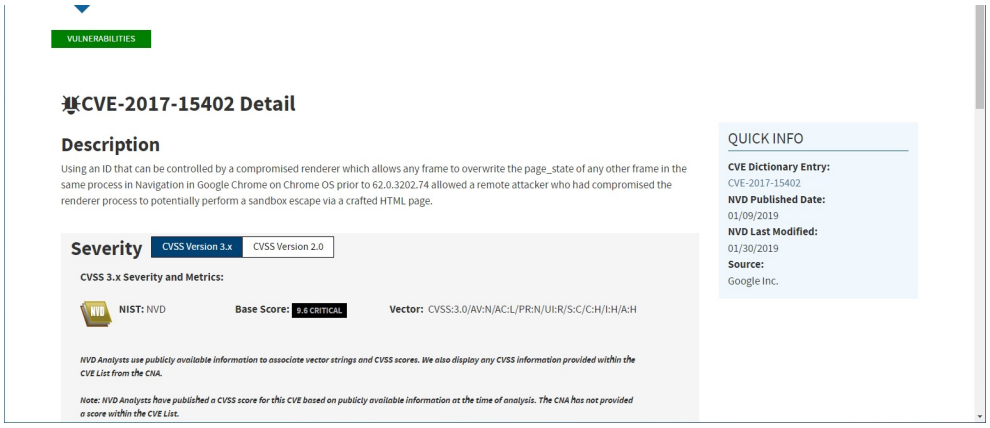
- Go to *Asset Identity Center* > *Asset Identity List* > *Asset List* to view *OT/IoT Vulnerabilities* in the table.



- Click the numbers in the *OT/IoT Vulnerabilities* column to display the vulnerabilities in more detail, including *Type*, *Severity*, *Reference*, and *Description*.



- Click the CVE reference in the *Reference* column to view the details.



- In the FortiAnalyzer CLI, you can enter the following command to check the status of the endpoint data link between FortiAnalyzer and FortiGate:

```
diagnose test application oftpd 20 fgt-stat
```

OT Purdue Model in a consolidated Asset & Identity Center Dashboard

This information is also available in the FortiAnalyzer 7.4 Administration Guide:

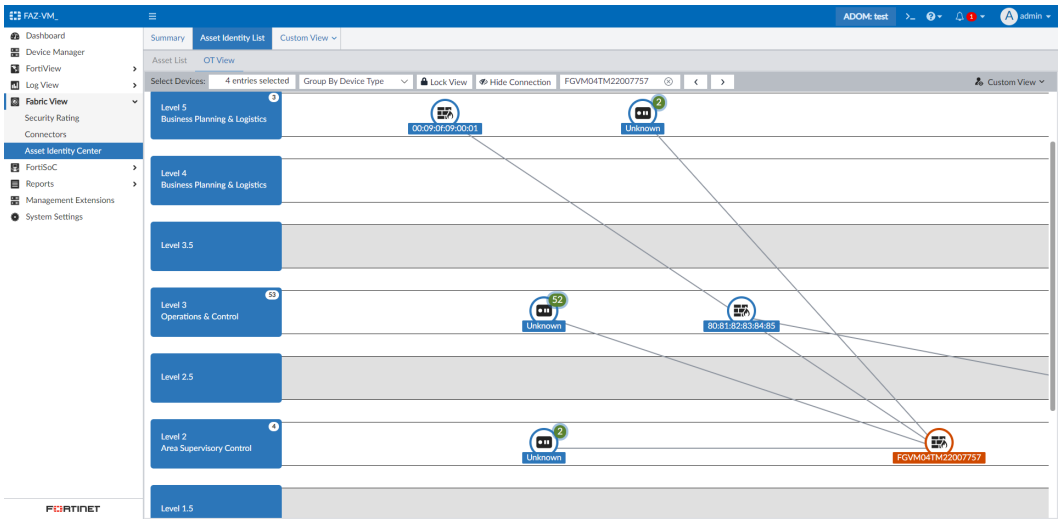
- OT View

An OT Purdue model has been added to a new and consolidated *Asset & Identity Center*.

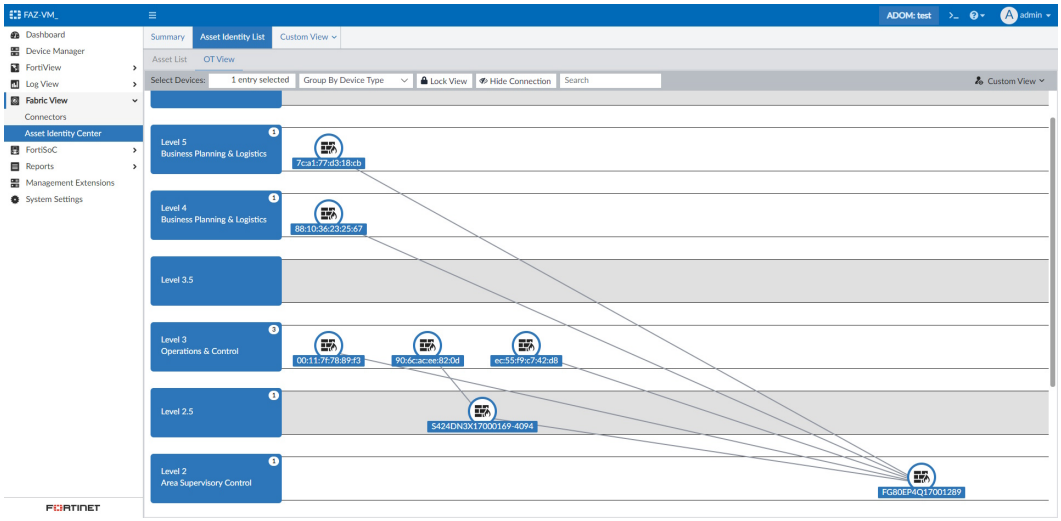
This spec introduces a consolidated dashboard for both Assets and Identities: *Fabric View* > *Asset Identity Center*. In previous versions, Asset and Identity each had a separate dashboard.

In the new *OT View*, each asset is represented in its corresponding Purdue Layer. All associated endpoints are visible with clear, linear relationships.

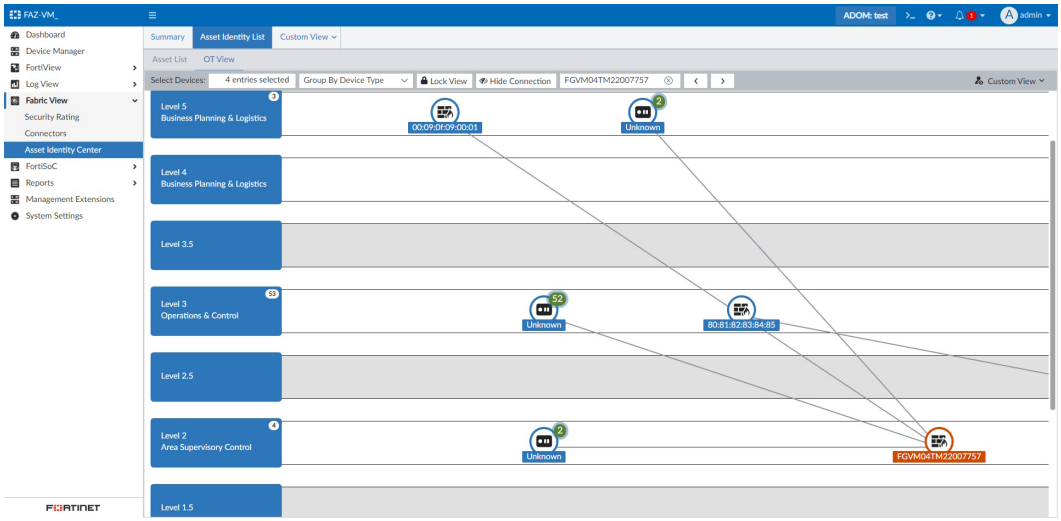
To view the new *OT View*, go to *Fabric View* > *Asset Identity Center* > *OT View*.



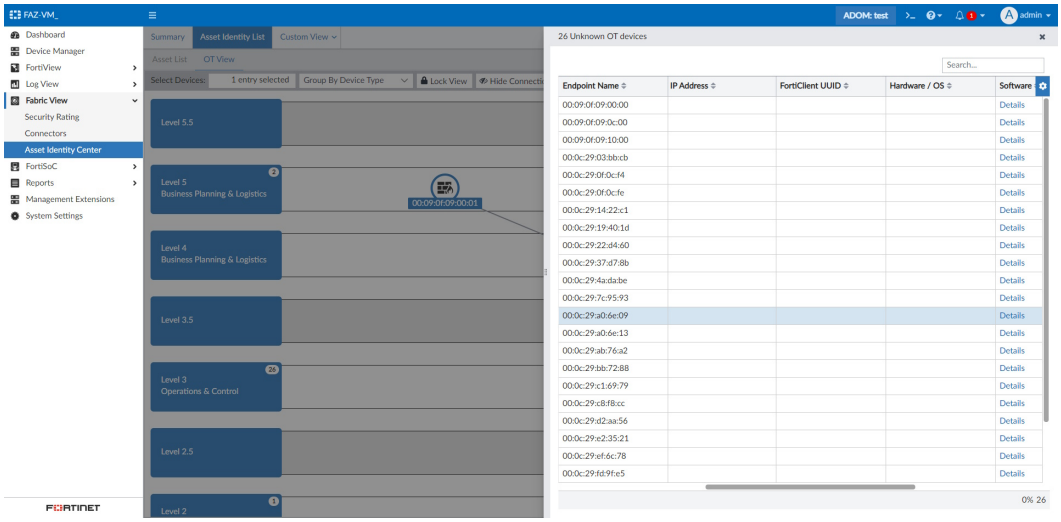
Use the *Select Devices* fields to display all endpoints associated with specified devices.



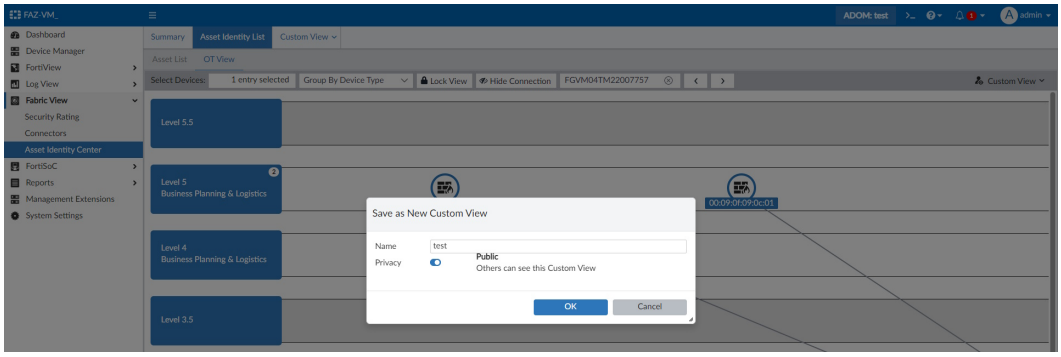
Use the *Search* field to find a specific endpoint, as needed.



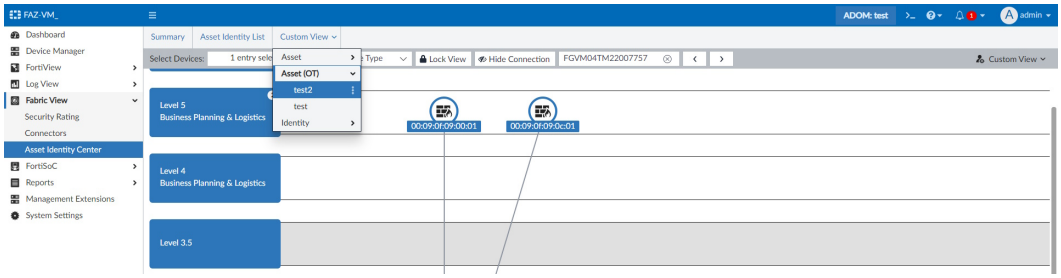
Click an endpoint to review the details of the endpoint or the endpoint's group.



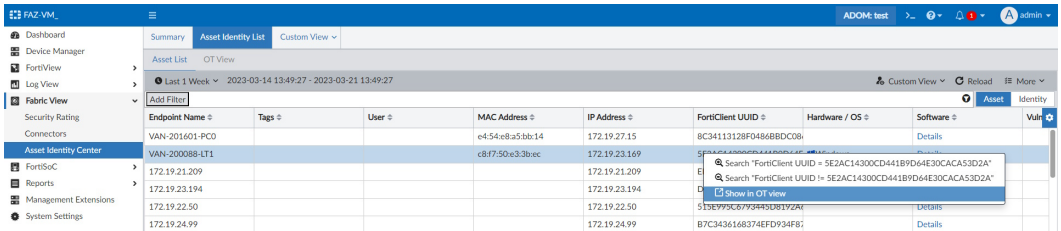
Within the *OT View* pane, click *Custom View* > *Save As Custom View* to create a custom view.



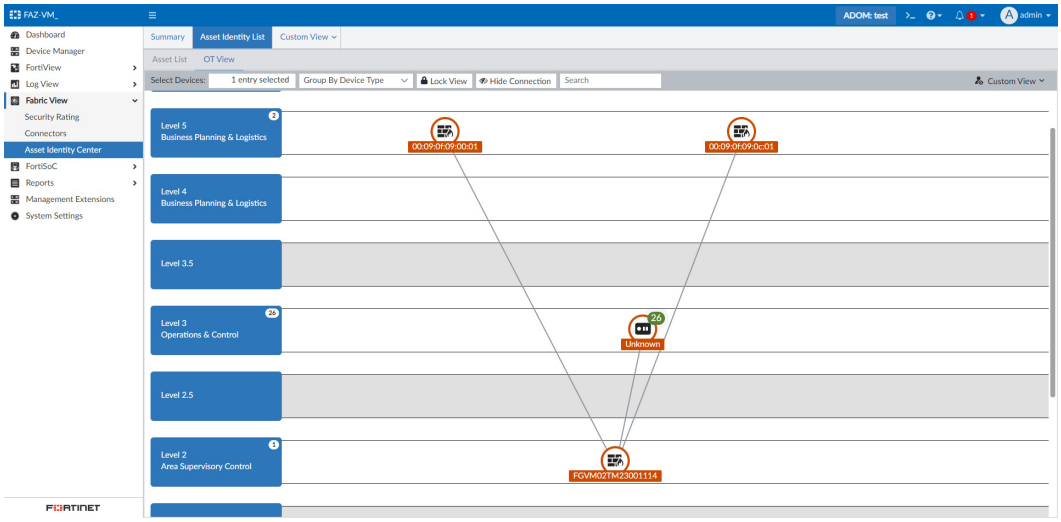
The saved custom views are available in *Fabric View* > *Asset Identity Center* > *Custom View*.



When using *Fabric View* > *Asset Identity Center* > *Asset List*, you can right-click an endpoint and click *Show in OT view* to display it in the OT view instead of the asset list.



After clicking *Show in OT* view, the *Fabric View* > *Asset Identity Center* > *OT View* opens to display the selected endpoint.

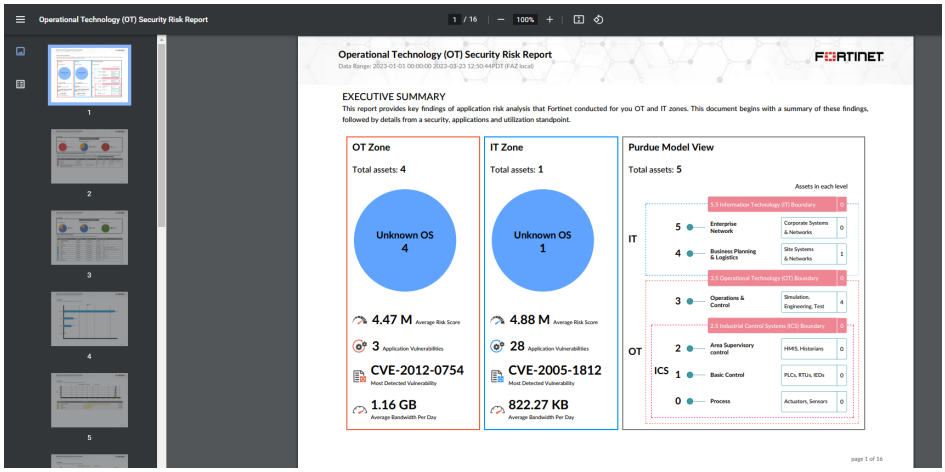


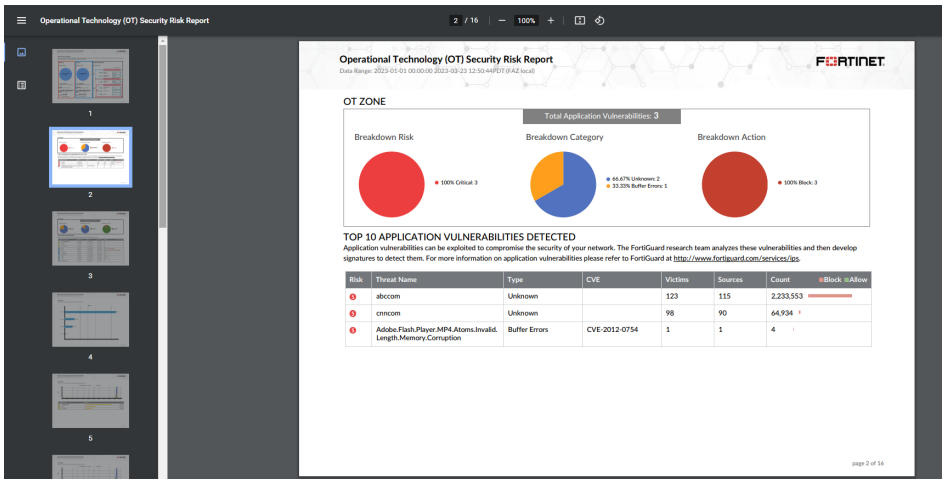
OT Security Risk Report

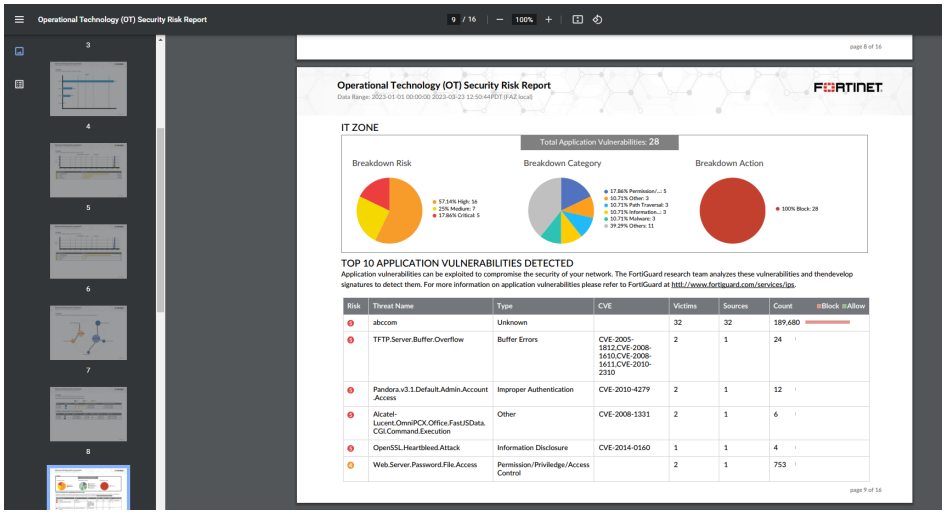
An *Operational Technology (OT) Security Risk Report* has been added to provide:

- Application risk analysis for OT and IT zones
- Blind-spot and hidden risks detection
- Purdue Model asset mapping

For example, see a sample of the report in PDF format below:

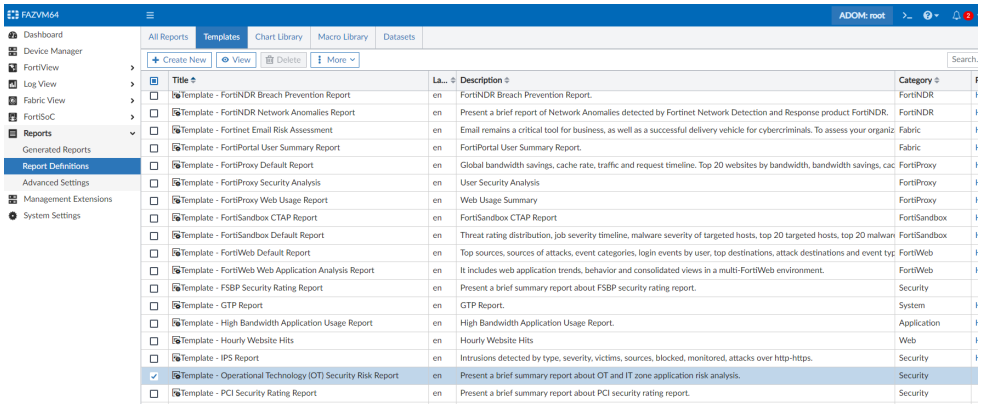






To create the report from the template:

1. Go to *Reports* > *Report Definitions* > *Templates*.
   From the *Preview* column, you can click *PDF* or *HTML* to preview the report in that format.
2. Select the checkbox for *Template - Operational Technology (OT) Security Risk Report*.



3. From the *More* dropdown, click *Create Report* to create a report using the template.
   You can also click *Clone* to clone the template and make adjustments.

To run the Operational Technology (OT) Security Risk Report:

1. Go to *Reports* > *Report Definitions* > *All Reports*, and double-click the row for the *Operational Technology (OT) Security Risk Report*.
   The *Edit: Operational Technology (OT) Security Risk Report* pane opens.
2. Click *Run Report*.
   Once the report is available, click the format to view the report in.

Index

The following index provides a list of all new features added to FortiAnalyzer 7.4. The index allows you to quickly identify the version where the feature first became available in FortiAnalyzer.

Select a version number to navigate in the index to the new features available for that release:

- 7.4.0 on page 82
- 7.4.1 on page 83

7.4.0

Fabric View

Connectors	• Webhook Connector to Support MS Teams on page 7

Security Operations

Asset and identity	• New charts in the Asset Identity Center on page 9
Other enhancements	• FortiSoC GUI reorganization on page 11

Log and Report

Logging	• FortiAnalyzer supports FortiWeb Cloud attack logs on page 16 • Support parsing and addition of third-party application logs to the SIEM DB on page 17 • Per-ADOM log rate on page 22
Log forwarding	• Fluentd support for public cloud integration on page 30
Reports	• Report guidance on page 34 • PCI Security Rating Report on page 36 • Cyber Threats Assessment Report update on page 37 • Threat Report update on page 38 • FSBP Security Rating Report on page 40 • CIS Controls Security Rating report on page 41 • Shadow IT Report on page 42
Other enhancements	• Time zone settings per ADOMs/Reports on page 46

System

Other enhancements	• FortiAnalyzer GUI enhancements on page 50 • Fabric of FAZ topology chart on page 54 • Fabric of FAZ: member authorization with supervisor on page 56 • Fabric of FAZ global FortiView support on page 61 • Fabric of FAZ: Central report support and creating Fabric groups on page 63 • Block out contract device from upgrading to next or major or minor release on page 66

Cloud Services

Cloud services	• FortiAnalyzer supports FortiCare Elite Service on page 70

Operational Technology

Operational Technology	• Operational Technology (OT) Security Service on page 74 • OT Purdue Model in a consolidated Asset & Identity Center Dashboard on page 76 • OT Security Risk Report on page 79

7.4.1

Security Operations

Other enhancements	• Notifications for new Outbreak Alerts 7.4.1 on page 14

Log and Report

Logging	• Support EMS multitenancy via FortiAnalyzer ADOMs 7.4.1 on page 24 • Logging support for FortiCASB 7.4.1 on page 26 • Logging support for FortiPAM 7.4.1 on page 28 • Logging support for FortiToken Cloud 7.4.1 on page 29
Reports	• FortiADC Report 7.4.1 on page 43 • Default ZTNA Report 7.4.1 on page 45

www.fortinet.com